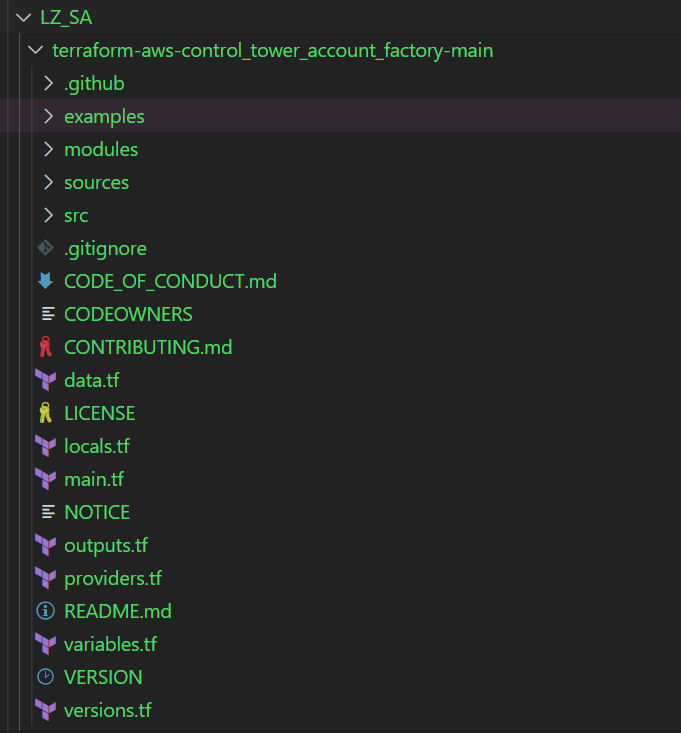
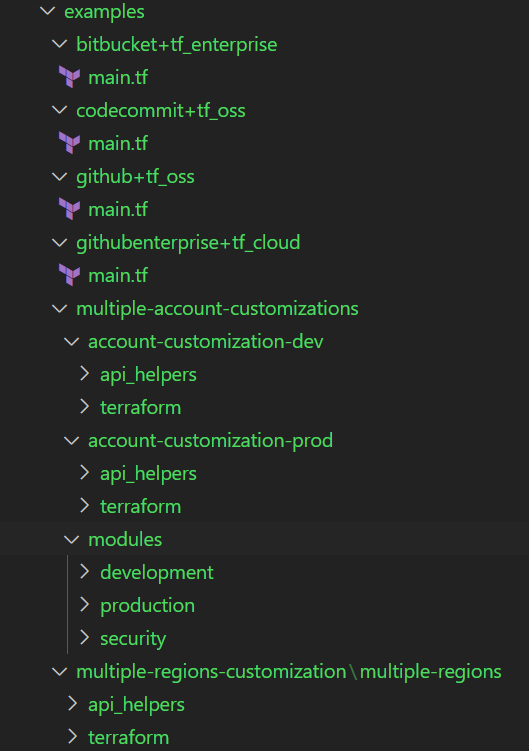
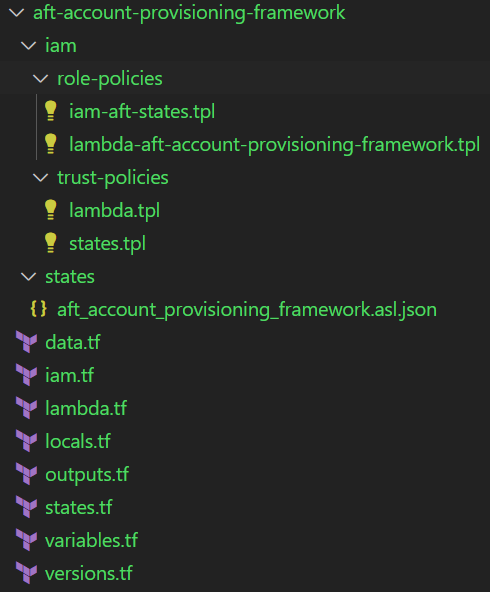
The Terraform language includes a few kinds of blocks for requesting or publishing named values.

* **Resource Block**: A resource block declares a resource of a given type with a given local name. The name is used to refer to this resource from elsewhere in the same Terraform module, but has no significance outside of the scope of a module.
* Variable: Input variable allowing users to customizate aspects of the configuration when used directly (e.g. via CLI, tfvars file or via environment variables), or as a module (via module arguments)
* [Output Values](https://www.terraform.io/language/values/outputs) are like return values for a Terraform module. Output value for consumption by another module or a human interacting via the UI.
* [Local Values](https://www.terraform.io/language/values/locals) are a convenience feature for assigning a short name to an expression. Terraform locals are named values that you can refer to in your configuration. You can use local values to simplify your Terraform configuration and avoid repetition. Local values (locals) can also help you write more readable configuration by using meaningful names rather than hard-coding values. Local values assigning names to expressions, so you can use these multiple times without repetition e.g., service\_name = "forum"
* **Versions**: You can also set a version constraint for each provider defined in the required\_providers block. The version attribute is optional, but we recommend using it to constrain the provider version so that terraform does not install a version of the provider that does not work with your configuration. If you do not specify a provider version, terraform will automatically download the most recent version during initialization.
* **Data Block**: A data block requests that Terraform read from a given data source and export the result under the given local name. The name is used to refer to this resource from elsewhere in the same Terraform module, but has no significance outside of the scope of a module.

**Root File Structure of git:**



* **terraform-aws-control\_tower\_account\_factory**  
  will be storing all the files.
  1. **.github** :  
     it has pull request file  
     
  2. **examples**:  
     it contains some organizational based examples to setup the account for dev and prod with some predefined modules for the same.  
     
  3. **Modules**:  
     - **aft-account-provisioning-framework**  
     

|  |  |
| --- | --- |
| **IAM** | 1. role-policies - iam-aft-states.tpl  - IAM aft policies for states and allow and deny rule with effect.   - lambda-aft-account-provisioning-framework.tpl  - Lambda aft policy for framework resources 2. trust-policies  - lambda and states.tpl  - it has the allow property for lambda and states services to be used via sts:Assume role. |
| **States** | it has json state of the aft framework for aft-account-provisioning-framework. |
| **data.tf** | IAM is using this data methods for resource creation with the help of role-based policy. |
| **Iam.tf** | IAM.tf is performing various tasks like invoke\_aft\_account\_provisioning\_framework, inside this it is using various data sets to create and attach the tags to resources: 1. Validate Request Lambda Permissions  2. Get Account Info Lambda Permissions  3. Create Role Lambda Permissions  4. Tag Account Lambda Permissions  5. Persist Metadata Lambda Permissions  6. states\_execution\_role |
| **Lambda.tf** | It is creating functions for the following: ### VALIDATE REQUEST FUNCTION  ### GET ACCOUNT INFO FUNCTION  ### CREATE ROLE FUNCTION  ### TAG ACCOUNT FUNCTION ### PERSIST METADATA FUNCTION  ### Account Metadata SSM Function  It is using various things like roles, variables etc to create and execute the functions. |
| **Locals.tf** | Locals is taking data from data.tf for lambda execution role. |
| **Outputs.tf** | It will provide the details of the given resources that are being created in account, Now, the output basically contains all the output attributes that you might have set in your TF: state\_machine\_arn, validate\_request\_function\_arn  get\_account\_info\_function\_arn, create\_role\_function\_arn,  tag\_account\_function\_arn, persist\_metadata\_function\_arn |
| **States.tf** | This is using lambda resources as locals and it is creating an aws\_sfn\_state\_machine resource. |
| **Variables.tf** | This contains all the required variables that are going to be used to execute the **aft-account-provisioning-framework** module with type. |
| **Versions.tf** | It is maintaining the versions of terraform binary and hashicorp aws provider as well. (It is required) |

- **aft-account-request-framework**   
This module deploys the components responsible for processing an account request. Functionality includes:

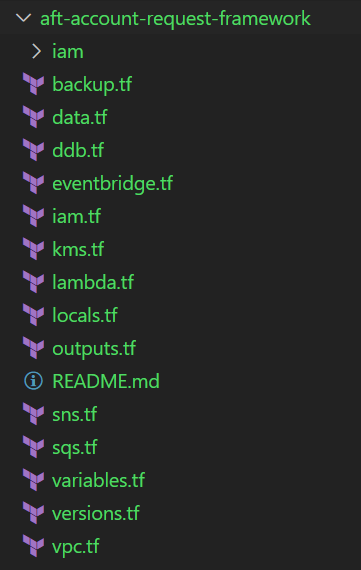
- Creating an audit for account requests/updates in the DynamoDB audit table

- Decision logic on whether a Service Catalog/Control Tower API call is needed

- Queueing Service Catalog requests by leveraging an SQS queue

- Forwarding and storing Control Tower events from the ct-management account into a DynamoDB table

- Triggering Step Functions based on a request payload

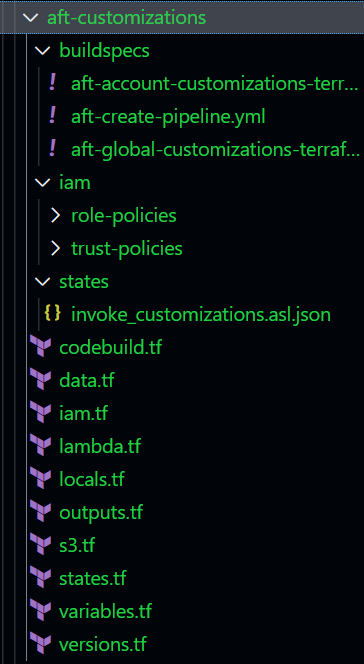


|  |  |
| --- | --- |
| IAM |  |
| Backup.tf |  |
| Data.tf |  |
| Ddb.tf |  |
| Eventbridge.tf |  |
| Iam.tf |  |
| Kms.tf |  |
| Lambda.tf |  |
| Locals.tf |  |
| Outputs.tf |  |
| Sns.tf |  |
| Sqs.tf |  |
| Variables.tf |  |
| Versions.tf |  |
| Vpc.tf |  |

* **aft-code-repositories**  
    
  

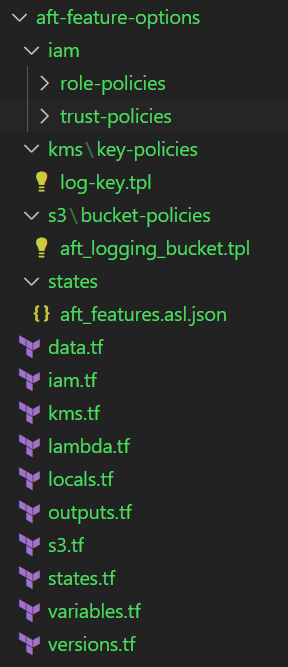
|  |  |
| --- | --- |
| buildspecs | These files are used in codebuild.tf file. |
| iam |  |
| Codebuild.tf | It is creating the resources list below:   * "aws\_codebuild\_project" "account\_request" - Job to apply Terraform for Account Requests * "aws\_codebuild\_project" "account\_provisioning\_customizations\_pipeline" - Deploys the Account Provisioning Customizations terraform project * "aws\_cloudwatch\_log\_group" "account\_request" * "aws\_cloudwatch\_log\_group" "account\_provisioning\_customizations" |
| Codecommit.tf |  |
| Codepipeline.tf |  |
| Codestar.tf | It is creating resources by taking reference of locals.tf and variables.tf  - "aws\_codestarconnections\_connection" "bitbucket"   * "aws\_codestarconnections\_connection" "github" * "aws\_codestarconnections\_connection" "githubenterprise" * "aws\_codestarconnections\_host" "githubenterprise" |
| Data.tf | Check the top Discussion |
| Iam.tf | It is creating roles for the following:   * # CodePipeline Roles  - "aws\_iam\_role" "account\_request\_codepipeline\_role"  - /iam/trust-policies/codepipeline.tpl  - "aws\_iam\_role\_policy" "account\_request\_codepipeline\_policy"  - /iam/role-policies/ct\_aft\_account\_request\_codepipeline\_policy.tpl  - "aws\_iam\_role" "account\_provisioning\_customizations\_codepipeline\_role"  - /iam/trust-policies/codepipeline.tpl  - "aws\_iam\_role\_policy" "account\_provisioning\_customizations\_codepipeline\_policy"  - /iam/role-policies/ct\_aft\_account\_provisioning\_customizations\_codepipeline\_policy.tpl * # Codebuild Role  - "aws\_iam\_role" "account\_provisioning\_customizations\_codebuild\_role"  - /iam/trust-policies/codebuild.tpl  - "aws\_iam\_role\_policy" "account\_provisioning\_customizations\_codebuild\_policy"  - /iam/role-policies/ct\_aft\_codebuild\_policy.tpl  - "aws\_iam\_role\_policy" "terraform\_oss\_backend\_account\_provisioning\_customizations\_codebuild\_policy"  - /iam/role-policies/ct\_aft\_codebuild\_oss\_backend\_policy.tpl  - "aws\_iam\_role" "account\_request\_codebuild\_role"  - /iam/trust-policies/codebuild.tpl  - "aws\_iam\_role\_policy" "account\_request\_codebuild\_policy"  - /iam/role-policies/ct\_aft\_codebuild\_policy.tpl  - "aws\_iam\_role\_policy" "terraform\_oss\_backend\_account\_request\_codebuild\_policy"  - /iam/role-policies/ct\_aft\_codebuild\_oss\_backend\_policy.tpl * # CloudWatch Events Role  - "aws\_iam\_role" "cloudwatch\_events\_codepipeline\_role"  - /iam/trust-policies/events.tpl  - "aws\_iam\_role\_policy" "cloudwatch\_events\_codepipeline\_role"  - /iam/role-policies/ct\_aft\_cwe\_policy.tpl   It is using variables.tf, data.tf, locals.tf. |
| Locals.tf | Check the top Discussion |
| Outputs.tf | Check the top Discussion  It is giving output of the codestar connection arn, by using locals.tf for the reference namce. |
| S3.tf | There is nothing in S3.tf file |
| Variables.tf | This contains all the required variables that are going to be used to execute the **aft-code-repositories module** with type. |
| Versions.tf | It is maintaining the versions of terraform binary and hashicorp aws provider as well. (It is required) |

* **aft-customizations**



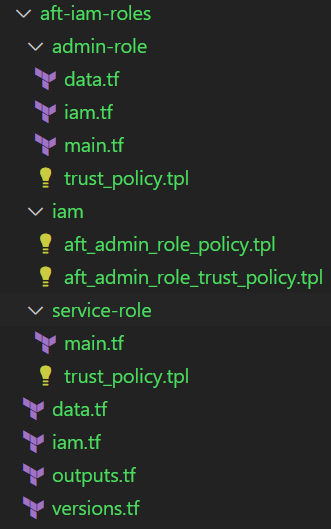
|  |  |
| --- | --- |
| buildspecs | It has yaml code for the account customisation, global customisattion and to create a pipeline |
| iam | It has IAM trust and role-based policy |
| states | It has invoke\_customisation code to manage states |
| codebuild.tf | This is creating 3 codebuild projects:   * # AFT Global Customizations Terraform * # AFT Account Customizations Terraform * # AFT Account Provisioning Framework SFN - aft-create-pipeline |
| Data.tf | Check the top discussion It is accessing some files from buildspecs:  data "local\_file" "aft\_global\_customizations\_terraform" {  filename = "${path.module}/buildspecs/aft-global-customizations-terraform.yml"  }    data "local\_file" "aft\_account\_customizations\_terraform" {  filename = "${path.module}/buildspecs/aft-account-customizations-terraform.yml"  }    data "local\_file" "aft\_create\_pipeline" {  filename = "${path.module}/buildspecs/aft-create-pipeline.yml"  } |
| Iam.tf | Creating the IAM resources for the following:   * # CodePipeline IAM Resources - aft\_codepipeline\_customizations\_role  - /iam/trust-policies/codepipeline.tpl - aft\_codepipeline\_customizations\_policy  - /iam/role-policies/aft\_codepipeline\_customizations\_policy.tpl * # CodeBuild IAM Resources - aft\_codebuild\_customizations\_role  - /iam/trust-policies/codebuild.tpl - aft\_codebuild\_customizations\_policy  - /iam/role-policies/aft\_codebuild\_customizations\_policy.tpl * # Step Functions - Invoke Customizations - aws\_iam\_role" "aft\_invoke\_customizations\_sfn"  - /iam/trust-policies/states.tpl - "aws\_iam\_role\_policy" "aft\_invoke\_customizations\_sfn"  - /iam/role-policies/aft\_states\_invoke\_customizations\_policy.tpl * # Lambda - Identify Targets - "aws\_iam\_role" "aft\_customizations\_identify\_targets\_lambda"  - /iam/trust-policies/lambda.tpl - "aws\_iam\_role\_policy" "aft\_identify\_targets\_lambda"  - /iam/role-policies/aft\_identify\_targets\_lambda.tpl - "aws\_iam\_role\_policy\_attachment" "aft\_identify\_targets\_lambda" * # Lambda - Execute Pipeline - "aws\_iam\_role" "aft\_customizations\_execute\_pipeline\_lambda"  - /iam/trust-policies/lambda.tpl - "aws\_iam\_role\_policy" "aft\_execute\_pipeline\_lambda"  - /iam/role-policies/aft\_execute\_pipeline\_lambda.tpl - "aws\_iam\_role\_policy\_attachment" "aft\_execute\_pipeline\_lambda" * # Lambda - Get Pipeline Executions - "aws\_iam\_role" "aft\_customizations\_get\_pipeline\_executions\_lambda"  - /iam/trust-policies/lambda.tpl - "aws\_iam\_role\_policy" "aft\_get\_pipeline\_executions\_lambda"  - /iam/role-policies/aft\_get\_pipeline\_status\_lambda.tpl - "aws\_iam\_role\_policy\_attachment" "aft\_get\_pipeline\_executions\_lambda" - "aws\_iam\_role\_policy" "terraform\_oss\_backend\_codebuild\_customizations\_policy"  - /iam/role-policies/ct\_aft\_codebuild\_oss\_backend\_policy.tpl |
| Lambda.tf | Creating lambda functions for the below resources:  # customizations\_identify\_targets   * aft\_customizations\_identify\_targets * “aws\_cloudwatch\_log\_group" "aft\_customizations\_identify\_targets"   # customizations\_execute\_pipeline   * "aws\_lambda\_function" "aft\_customizations\_execute\_pipeline" * "aws\_cloudwatch\_log\_group" "aft\_execute\_pipeline"   # customizations\_get\_pipeline\_executions   * "aws\_lambda\_function" "aft\_customizations\_get\_pipeline\_executions" |
| Locals.tf | Check the top Discussion |
| Outputs.tf | Check the top Discussion |
| S3.tf | It is creating buckets for the following resources:   * resource "aws\_s3\_bucket" "aft\_codepipeline\_customizations\_bucket" { * bucket = "aft-customizations-pipeline-${data.aws\_caller\_identity.current.account\_id}" * } * resource "aws\_s3\_bucket\_versioning" "aft-codepipeline-customizations-bucket-versioning" { * bucket = aws\_s3\_bucket.aft\_codepipeline\_customizations\_bucket.id * versioning\_configuration { * status = "Enabled" * } * } * resource "aws\_s3\_bucket\_server\_side\_encryption\_configuration" "aft-codepipeline-customizations-bucket-encryption" { * bucket = aws\_s3\_bucket.aft\_codepipeline\_customizations\_bucket.id * rule { * apply\_server\_side\_encryption\_by\_default { * kms\_master\_key\_id = var.aft\_kms\_key\_id * sse\_algorithm = "aws:kms" * } * } * } * resource "aws\_s3\_bucket\_acl" "aft-codepipeline-customizations-bucket-acl" { * bucket = aws\_s3\_bucket.aft\_codepipeline\_customizations\_bucket.id * acl = "private" * } |
| States.tf | It has created a local's resource block for the names and that names are imported from data, lambda functions and variables -> /states/invoke\_customizations.asl.json |
| Variable.tf | This contains all the required variables that are going to be used to execute the **aft-customizations module** with type. |
| Versions.tf | It is maintaining the versions of terraform binary and hashicorp aws provider as well. (It is required) |

- **aft-feature-options**

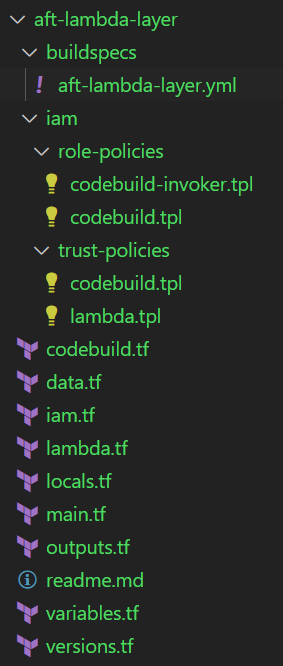


|  |  |
| --- | --- |
| iam | Role-policies   * aft\_features\_states.tpl: it has a policy to perform action for sns and lambda invoke. * aft\_enroll\_support.tpl: it has a policy to perform action for ssm, kms, sts, and sns. * aft\_enable\_cloudtrail.tpl: it has a policy to perform action for ssm, kms, sts, and sns. * aft\_delete\_default\_vpc\_lambda.tpl : it has a policy to perform action for EC2, ssm, kms, sts, and sns.   Trust-policies- it has sts assume role policy for lambda and states. |
| KMS | It has policy to accept the services for delivery-logs, vpc-flow-logs, cloudtrail logs + enable IAM user permission for root. |
| S3 | It is having policy for S3 to allot permission to perform and create the resources. |
| states | It is having states for states.tf |
| Data.tf | Check the top discussion |
| Iam.tf | Some certain resources/task being performed in IAM:   * # Step Functions - AFT Features  Policy: - /iam/trust-policies/states.tpl - /iam/role-policies/aft\_features\_states.tp * # Lambda - Delete Default VPC Policy: - /iam/trust-policies/lambda.tpl - /iam/role-policies/aft\_delete\_default\_vpc\_lambda.tpl * # Lambda - Enroll Support Policy: - /iam/trust-policies/lambda.tpl - /iam/role-policies/aft\_enroll\_support.tpl * # Lambda - Enable Cloudtrail Policy: - /iam/trust-policies/lambda.tpl - /iam/role-policies/aft\_enable\_cloudtrail.tpl |
| Kms.tf | KMS key for encrypt/decrypt log files  It is using the policy-> /kms/key-policies/log-key.tpl |
| Lambda.tf | It is creating some lambda function for the below listed resources:   * aft\_delete\_default\_vpc * aft\_enroll\_support * aft\_enable\_cloudtrail |
| Locals.tf | Check Top discussion |
| outputs.tf | Check Top discussion |
| S3.tf | It is creating some resource listed below:   * aft\_logging\_bucket * aft\_logging\_bucket\_logging * aft\_logging\_bucket\_versioning * aft\_logging\_bucket\_encryption * aft\_logging\_bucket\_lifecycle\_configuration * aft\_logging\_bucket * aft\_access\_logs * aft\_access\_logs\_versioning * aft\_access\_logs\_encryption * aft\_access\_logs\_lifecycle\_configuration * aft\_access\_logs\_acl |
| States.tf | It is accessing -> /states/aft\_features.asl.json, roles as well,Lambda.tf, and variable.tf  aft\_features.asl.json - it is deleting the default VPC, and enrolling into the enterprise support by enabling the cloudtrail for success and failure notification. |
| Variables.tf | This contains all the required variables that are going to be used to execute the **aft-feature-options** module with type. |
| Versions.tf | It is maintaining the versions of terraform binary and hashicorp aws provider as well. (It is required) |

- **aft-iam-roles**



|  |  |
| --- | --- |
| Admin-role | 1. Data.tf - aws partition will be readed and exported from here 2. Main.tf - it has terraform provider. 3. Iam.tf - Iam have variables and it is creating a role with name “AWSAFTExecution”  - and attaching the administrator access to role in another resource. - and giving output of the arn. 4. Trust-policy - it has sts:AssumeRole policy. |
| iam | It has trust policy for Iam roles. |
| Service-role | 1. Main.tf - it has terraform provider - it has variable declared - it is creating a role and assigning administrator access to that role 2. Trust-policy - sts:AssumeRole role policy |
| Data.tf | Check the previous discussion. |
| Iam.tf | It is creating roles by using the iam folder policy and iam admin policy and it is also using some modules as well. |
| Outputs.tf | Check the previous discussion. |
| Versions.tf | It is maintaining the versions of terraform binary and hashicorp aws provider as well. (It is required)  it is using configuration\_aliases alias, for using the same provider with different configurations for different resources; version, which we no longer recommend (use provider requirements instead) Unlike many other objects in the Terraform language, a provider block may be omitted if its contents would otherwise be empty. Terraform assumes an empty default configuration for any provider that is not explicitly configured. |

- **aft-lambda-layer**  
 

|  |  |
| --- | --- |
| **buildspecs** | **- aft-lambda-layer.yml** it contains configuration file, and some commands to execute. |
| **iam** | It has role and trust-based policy for the lambda layer with codebuild |
| **Codebuild.tf** | It is creating a resource of Codebuild project to create lambda layer |
| **Data.tf** |  |
| **Iam.tf** | It is creating the roles for codebuild and attaching the policy to that role. Taking details from variables, locals, and data.tf files. |
| **Lambda.tf** | It is creating a resource of lambda and assigning the role and the function to perform the task, and also it is configuring the VPC as well. It will give an output of the resource build status. |
| **Locals.tf** | Check the top Description |
| **Main.tf** | Creating the resources for the lambda layer, is the main execution file for the **aft-lambda-layer.** |
| **Outputs.tf** | Check the top Description |
| **Variables.tf** | This contains all the required variables that are going to be used to execute the **aft-lambda-layer** module with type. |
| **Versions.tf** | It is maintaining the versions of terraform binary and hashicorp aws provider as well. (It is required) |

**# Python Layer Builder**

Python Layer Builder deploys a codebuild job which creates an AWS Lambda Layer version from a github repository.

This project deploys an IAM role, S3 bucket, Codebuild project, and Cloudwatch Event which triggers the codebuild project.

The codebuild project runs `pip install` using the specified version of python and installs the required packages to a virtual environment,

It then zips the python/lib/pythonx.x folder, and uploads it to S3.

Terraform then waits for approximately 3 minutes and attempts to create a lambda layer from this S3 bucket and key.

If no object is found at this location, the Terraform apply will fail. If this is an update, and something goes wrong with the buid process, the terraform apply will not record any errors. You are encouraged to impement error-handling notifications and integrate them with the python-layer-builder installation in your environment.

**# Requirements File**

The build process expects a python package list at the location: `./layer/requirements.txt`

**# Variables**

layer\_name - the name of the lambda layer

aws\_region - the region to deploy the layer in

source\_url - the url of the github repository which contains the ./layer/ folder, custom packages, and requirements.txt

source\_branch - the branch to clone from the source repository.

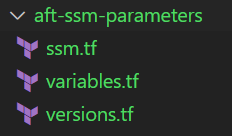
source\_type - Currently, only GITHUB has been tested.

lambda\_layer\_python\_version - Major python version. Defaults to 3.9

github\_token - Set $TF\_VAR\_github\_token to securely configure this variable with a personal access token to github.

**# Outputs**

layer\_version\_arn - the ARN of the lambda layer version

**- aft-ssm-parameters**  


|  |  |
| --- | --- |
| Ssm.tf | It is using variables and creating resources for SSM like request queue, request table, events etc. |
| Variables.tf | This contains all the required variables that are going to be used to execute the **aft-ssm-parameters** module with type. |
| Versions.tf | It is maintaining the versions of terraform binary and hashicorp aws provider as well. (It is required) |