# Baseline deployment – technical details

## Purpose of the documentation

This document shows the details of the creation of new accounts, and deployment of the baseline on these accounts. The account provides details on the used technologies and documents the steps. The design of the baseline deployment is focused on serverless aproach, with multiple layer, which allowing us, to easily modify functions under the public interface.

## Used technologies

Lambda: Lambda service is provided by AWS. This is the main product of the serverless aproach what we are using. Lambda allows to execute codes written in Node.js,Java,Python,.Net core, Go. All of our codes written in python 3.6. Details can bound: <https://aws.amazon.com/lambda/>

Step functions: Step functions are used, to coordinate the running of several steps (lambda functions) as a workflow. Step functions can be used by writing the workflow in json (Amazon States Language <https://docs.aws.amazon.com/step-functions/latest/dg/concepts-amazon-states-language.html>) . This helps to eliminate the cost of long running python codes (by checking it in a defined interval). More details can be found at: <https://aws.amazon.com/step-functions/>

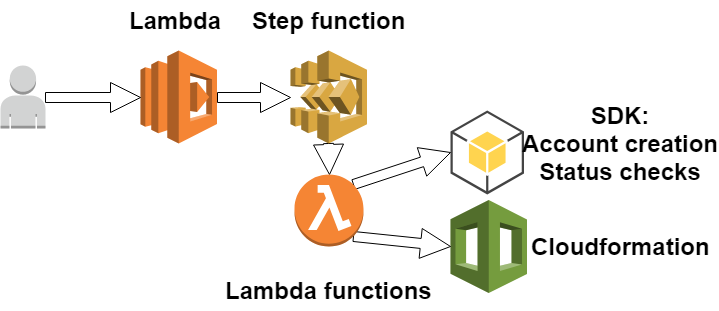
S3: S3 is an object storage provided by AWS. We are using S3 buckets to store Type A, and Type B account status. Also we will extend the current workflow to store status on s3 buckets. Also we are storing cloudformation templates ont he s3 buckets. More details about s3 can be found at: <https://aws.amazon.com/s3/>

Cloudformation: Cloudformation is used to deploy the baseline objects (currently IAM policies, roles, Cloudtrail configuration),. All of the attached accounts have by this the same managed objects. The cloudformation templates are ’Baseline-PROD’ and ’SecurityAlert-PROD’.

## Interface with the OSS :

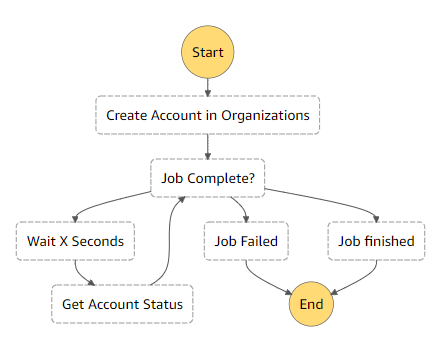
For OSS a lambda function provided (arn:aws:lambda:eu-central-1:275662325630:function:createAccount) which is the main entry point in our process. The interface is documented and developed. The OSS team calling this function whenever a new order is processed. This lambda function is used to start processes, and query for status of the process by providing the operation\_id. This lambda function either creates a file on S3 bucket (for TYPE A, and TYPE B), or starts a State Machine(Step function) execution with the provided parameters. For details on this interface, please refer to the OSS interface documentation (\* doc name\* )

## Interface and connected services during the baseline deployment:



### Account creation:

The interface can be executed via lambda. Lambda takes the parameters as json payload, and depends on the task it will query for the status, or will launch the workflow which is a call to step function arn:aws:states:eu-central-1:275662325630:stateMachine:createNewAccount . The step machine invokes lambda function arn:aws:lambda:eu-central-1:275662325630:function:createAccountInOrganizations:PROD , which tries to create the account within our organization with the provided inputs. The account creation process is then monitored by the function arn:aws:lambda:eu-central-1:275662325630:function:getAccountStatus . Depends ont he output of the call it will fail, or will call the the lambda function arn:aws:lambda:eu-central-1:275662325630:function:deployProvision.



### Deployment of the current baseline:

Af the process finished, and the account is created, the final step of this state machine is to execute lambda function arn:aws:lambda:eu-central-1:275662325630:function:deployProvision which invokes the step function arn:aws:states:eu-central-1:275662325630:stateMachine:PROD-Provision\_Baseline\_Release\_1 . This invokes several lambda functions, which deployes the mandatory roles needed for cloudformation, and also it deploys the unmanaged items like s3 dpc policy, or groups, and roles.

### Parts of the step function baseline prod:

Baseline PROD step function runs several lambda functions described as following:

#### arn:aws:lambda:eu-central-1:275662325630:***function***:provisionIamAdmin :

Creates Cloudformation role ont he account. For this trust relationship must be in place with role named TSI\_Base\_FullAccess.

Input parameters: accountId  
Creates: AWSCloudFormationStackSetExecutionRole role  
Output: response of create\_role function (<https://boto3.readthedocs.io/en/latest/reference/services/iam.html#IAM.Client.create_role> )

#### arn:aws:lambda:eu-central-1:275662325630:function:createPasswordPolicy

Configures password policy on the target account.

Input parameters: accountId  
Creates: Password policy configuration on the target account  
Output: AccountPasswordPolicy.update function (<https://boto3.readthedocs.io/en/latest/reference/services/iam.html#IAM.AccountPasswordPolicy.update> )

#### arn:aws:lambda:eu-central-1:275662325630:function:AddEventBusOnSecDevOp

Configures eventbus ont he secdevops account (optionally accepts different secDevopsArn as secdevops accountid)

Input parameters: accountId, sevDevopsArn (optionally)  
Creates: Entry in eventbus to accept messages from customer account  
Output: None

#### arn:aws:lambda:eu-central-1:275662325630:function:addAccountCWDPCRule

Configures cloudwatch event rule name ’S3\_DPC\_Enforce\_Basline’ in sevdevops account

Input: accountId, secDevopsArn (optionally)  
Creates: New line int he rule to include the accountid of the target account  
Output:None

#### arn:aws:lambda:eu-central-1:275662325630:function:addCloudTrailPolicy

Configures s3 bucket bucket policy on secdevops. Allows cloudtrail to create json files in the bucket, coming from customer account.

Input: accountId  
Creates: New line int he bucket policy in s3 bucket  
Output: String (Found, or Added Permission)

#### arn:aws:lambda:eu-central-1:275662325630:function:createCloudFormationInstance

Creates cloudformation stack instance on the target account. Both Baseline-PROD, and SecurityAlert-Prod are using this currently (this will be changed).  
Input: accountId, email (for SecurityAlert-PROD only)  
Creates: Stack instance, which creates several objects ont he target account  
Output: create\_stack\_instance function response (<https://boto3.readthedocs.io/en/latest/reference/services/cloudformation.html#CloudFormation.Client.create_stack_instances>)

#### arn:aws:lambda:eu-central-1:275662325630:function:createAdminUser

Creates the first IAM user with the requested name, sends out email with login information to the requested email address.

Input: action (with value provision), accountId, username,email  
Creates: IAM user, password, login profile, email for the customer  
Output: password

#### arn:aws:lambda:eu-central-1:275662325630:function:createEncryptionKeys

Creates KMS encryption keys in all regions. One with alias TSI\_Base\_InternalS3Key, one with alias TSI\_Base\_ConfidentialS3Key.

Input: accountId  
Creates: two kms keys in all regions  
Output:None

#### arn:aws:lambda:eu-central-1:275662325630:function:addS3RulesOnCustomerAccount

Creates cloudwatch rule named TSI\_Base\_CW\_Rule\_S3\_ACL\_Send\_SecDevops ont he customer account. This rule forwards the s3 events to the secdevops eventbus. In all regions

Input: accountId  
Creates: CW Rules in all regions int he customer account  
Output: None