AWSTemplateFormatVersion: '2010-09-09'

Description: This template configures the AWS Account with the IDT Team Role

Metadata:

AWS::CloudFormation::Interface:

ParameterGroups:

- Label:

default: AWS Request Number Information

Parameters:

- pAWSRequestNumber

- Label:

default: Team Information

Parameters:

- pTeamName

- Label:

default: READ-ONLY Access Section

Parameters:

- pROAccessvalue

- pS3BucketROType

- pS3ReadOnlyBucketNames

- pS3ReadOnlyBucketNamePaths

- Label:

default: READ-WRITE Access Section

Parameters:

- pRWAccessvalue

- pS3BucketRWType

- pS3ReadwriteBucketNames

- pS3ReadwriteBucketNamePaths

Parameters:

pROAccessvalue:

Type: String

Description: "Do you need this access policy. I.e. true or false"

Default: true

AllowedValues:

- true

- false

pRWAccessvalue:

Type: String

Description: "Do you need this access policy. I.e. true or false"

Default: true

AllowedValues:

- true

- false

pS3BucketROType:

Type: String

Description: "Select the type of access. I.e. READ-ONLY or READ-WRITE"

Default: "READ-ONLY"

AllowedValues:

- READ-WRITE

- READ-ONLY

pS3BucketRWType:

Type: String

Description: "Select the type of access. I.e. READ-ONLY or READ-WRITE"

Default: "READ-WRITE"

AllowedValues:

- READ-WRITE

- READ-ONLY

pTeamName:

Type: String

Description: "Please select the Team who is requesting access to the S3 Bucket"

Default: CDM

AllowedValues:

- CDM

- CIA

- CloudAdmin

- CorporateApps

- DataGovernance

- DBA

- DS-Client

- EPM

- GA

- IDEA

- IDT

- InfoSec

- MarkitEDM

- Middleware

- TCS-CDM

# It makes sense to have this as a drop-down for folks to select from, however as more Buckets (and edge cases of Buckets) are created this could quickly get out of date

pS3ReadOnlyBucketNames:

Type: String

Description: "Input the Bucket Name and Path. Ex. The Bronze Bucket in DL-NP would be entered as: aci-dl-bronze-dev-48-us-east-2"

Default: "aci-48-dummy-bucket"

AllowedValues:

- aci-48-dummy-bucket

- aci-88-bucket

# It makes sense to have this as a drop-down for folks to select from, however as more buckets and root-level folders are created this could quickly get out of date

pS3ReadwriteBucketNames:

Type: String

Description: "Input the Bucket Name and Path. Ex. The Bronze Bucket in DL-NP would be entered as: aci-dl-bronze-dev-48-us-east-2"

Default: "aci-48-dummy-bucket"

AllowedValues:

- aci-48-dummy-bucket

- aci-88-bucket

pS3ReadOnlyBucketNamePaths:

Type: String

Description: "Input the Path from the root of the Bucket. Ex. The client folder would be entered as: /client"

Default: "/client"

AllowedValues:

- "/client"

- "/investment"

- "/product"

- "/licensed/datasource1" # This is just an example and is not an actual path

pS3ReadwriteBucketNamePaths:

Type: String

Description: "Input the Path from the root of the Bucket. Ex. The client folder would be entered as: /client"

Default: "/client"

AllowedValues:

- "/client"

- "/investment"

- "/product"

- "/licensed/datasource1" # This is just an example and is not an actual path

pAWSRequestNumber:

Type: String

Description: "Enter the AWS Request Number as documented in the Completed Requests Folder. Format - AWS-R#####"

MinLength: 1

MaxLength: 10

AllowedPattern: '^AWS\-R[0-9]{5}'

ConstraintDescription: "The AWS Request Number must be in the following format - AWS-R#####"

Mappings:

ACIAcctRefNumber:

'350730245305':

ACINum: '32'

ACIEnv: 'idt-nonprod'

ACIRolePrefix: 'AWS-IDT-NP'

'432616532185':

ACINum: '08'

ACIEnv: 'it-rnd'

'634670906551':

ACINum: '47'

ACIEnv: 'dl'

pBucketPrefix: 'aci-dl'

ACIRolePrefix: 'AWS-DL-P'

ACIKMSAliasPrefix: 'aci-aws'

'696272441511':

ACINum: '48'

ACIEnv: 'dl-nonprod'

pBucketPrefix: 'aci-dl-nonprod'

ACIRolePrefix: 'AWS-DL-NP'

'560337562992':

ACINum: '49'

ACIEnv: 'dl-qa'

pBucketPrefix: 'aci-dl-qa'

ACIRolePrefix: 'AWS-DL-QA'

'402834705600':

ACINum: '22'

ACIEnv: 'cdm-nonprod'

pBucketPrefix: 'aci-cdm-nonprod'

ACIRolePrefix: 'AWS-CDM-NP'

ACITeamName:

'CDM':

ACIIAMRoleName: "CDM-Access-Role"

ACITeamNameLower: 'cdm'

'CIA':

ACIIAMRoleName: "CIA-Access-Role"

ACITeamNameLower: 'cia'

'CloudAdmin':

ACIIAMRoleName: "CloudAdmin-Access-Role"

ACITeamNameLower: 'itcloud'

'DataGovernance':

ACIIAMRoleName: "DataGovernance-Access-Role"

ACITeamNameLower: 'datagovernance'

'DBA':

ACIIAMRoleName: "DBAdmin-Access-Role"

ACITeamNameLower: 'dba'

Conditions:

Accessresources: !Equals [ !Ref pROAccessvalue, false ]

ROResources: !Equals [ !Ref pS3BucketROType, READ-ONLY ]

RWResources: !Equals [ !Ref pS3BucketRWType, READ-WRITE ]

#NOResources: !Equals [ !Ref pS3BucketType, NONE ]

CreateROResources: !And

- !Equals [ !Ref pROAccessvalue, true ]

- !Condition ROResources

CreateRWResources: !And

- !Equals [ !Ref pRWAccessvalue, true ]

- !Condition RWResources

Resources:

S3DataAccessROPolicy:

Type: AWS::IAM::ManagedPolicy

Condition: CreateROResources

Description: This is a read-only bucket policy function

Properties:

Description: !Join

- ''

- - 'This Policy provisions READ-ONLY Access for the '

- !Ref pTeamName

- ' Team to access S3 Buckets and Objects. Provisioned as part of Request '

- !Ref pAWSRequestNumber

ManagedPolicyName:

'Fn::Join':

- '-'

- - !FindInMap

- ACIAcctRefNumber

- !Ref 'AWS::AccountId'

- ACIRolePrefix

- 'S3'

- !Ref pTeamName

- 'GenericDataAccess-RO-Policy'

PolicyDocument:

Version: "2012-10-17"

Statement:

- Sid: "AllowS3ConsoleAccess"

Effect: Allow

Action:

- s3:ListAllMyBuckets

Resource: "\*"

- Sid: "AllowS3ListBucketAccess"

Effect: Allow

Action:

- s3:ListBucket\*

- s3:GetBucketLocation

Resource:

- !Join [ "", [ "arn:aws:s3:::", !Ref "pS3ReadOnlyBucketNames" ] ]

- Sid: "AllowS3READONLYAccessToS3BucketAndObjects"

Effect: Allow

Action:

- s3:ListObjects

- s3:GetObject\*

Resource:

# This will grant access to the folder and nothing else inside the Bucket as intended

- !Join [ "", [ "arn:aws:s3:::", !Ref "pS3ReadOnlyBucketNames", !Ref "pS3ReadOnlyBucketNamePaths", "/\*" ] ]

S3DataAccessRORole:

Type: 'AWS::IAM::Role'

Condition: CreateROResources

Properties:

RoleName:

'Fn::Join':

- '-'

- - !FindInMap

- ACIAcctRefNumber

- !Ref 'AWS::AccountId'

- ACIRolePrefix

- 'RO'

- !FindInMap

- ACITeamName

- !Ref pTeamName

- ACIIAMRoleName

Description: !Join

- ''

- - 'This Role is attaching the S3 READ-ONLY Policy to the Access for the '

- !Ref pTeamName

AssumeRolePolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Principal:

Service:

- ec2.amazonaws.com

Action:

- 'sts:AssumeRole'

Path: /

ManagedPolicyArns:

- !Ref S3DataAccessROPolicy

S3DataAccessRWPolicy:

Type: AWS::IAM::ManagedPolicy

Condition: CreateRWResources

Description: This is a read-write bucket policy function

Properties:

Description: !Join

- ''

- - 'This Policy provisions READ-WRITE Access for the '

- !Ref pTeamName

- ' Team to S3 Buckets and Objects. Provisioned as part of Request '

- !Ref pAWSRequestNumber

ManagedPolicyName:

'Fn::Join':

- '-'

- - !FindInMap

- ACIAcctRefNumber

- !Ref 'AWS::AccountId'

- ACIRolePrefix

- 'S3'

- !Ref pTeamName

- 'GenericDataAccess-RW-Policy'

PolicyDocument:

Version: "2012-10-17"

Statement:

- Sid: "AllowS3ConsoleAccess"

Effect: Allow

Action:

- s3:ListAllMyBuckets

Resource: "\*"

- Sid: "AllowS3ListBucketAccess"

Effect: Allow

Action:

- s3:ListBucket\*

- s3:GetBucketLocation

Resource:

- !Join [ "", [ "arn:aws:s3:::", !Ref "pS3ReadwriteBucketNames" ] ]

- Sid: "AllowS3ReadWriteAccess"

Effect: Allow

Action:

- s3:\*

Resource:

# This will grant access to the folder and nothing else inside the Bucket as intended

- !Join [ "", [ "arn:aws:s3:::", !Ref "pS3ReadwriteBucketNames", !Ref "pS3ReadwriteBucketNamePaths", "/\*" ] ]

S3DataAccessRWRole:

Type: 'AWS::IAM::Role'

Condition: CreateRWResources

Properties:

RoleName:

'Fn::Join':

- '-'

- - !FindInMap

- ACIAcctRefNumber

- !Ref 'AWS::AccountId'

- ACIRolePrefix

- 'RW'

- !FindInMap

- ACITeamName

- !Ref pTeamName

- ACIIAMRoleName

Description: !Join

- ''

- - 'This Role is attaching the S3 READ-WRITE Policy to the Access for the '

- !Ref pTeamName

AssumeRolePolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Principal:

Service:

- ec2.amazonaws.com

Action:

- 'sts:AssumeRole'

Path: /

ManagedPolicyArns:

- !Ref S3DataAccessROPolicy

Outputs:

S3DataAccessROPolicyName:

Condition: CreateROResources

Value: !Ref S3DataAccessROPolicy

Description: S3 ro policy arn

S3DataAccessRORoleName:

Condition: CreateROResources

Value: !Ref S3DataAccessRORole

Description: S3 RO Role Name

S3DataAccessRWPolicyName:

Condition: CreateRWResources

Value: !Ref S3DataAccessRWPolicy

Description: S3 rw policy arn

S3DataAccessRWRoleName:

Condition: CreateRWResources

Value: !Ref S3DataAccessRWRole

Description: S3 RW Role Name

Good Morning Sai,

This would be done as I described in my previous email via unique IAM Policies for each “Type of Access”:

This would allow us to have a “Parameter Group” for READ-ONLY, WRITE-ONLY, READ-WRITE, etc. and if the top-level parameter which asks, “Is [TYPE OF ACCESS] needed?” is “No” we would set a Condition to be False for that Access and thereby not create the IAM Data Access Policy for that type of access. Conditions will only equate to “True” when done so in your “Conditions” Section of the CFT if the answer is “Yes”. Therefore, we would then create the IAM Data Access Policy for that type of access as the Condition is met for that Resource to be created.

Here is an example I did for the Hackathon’s with creating different KMS Keys based upon the type of IAM SVC Users which would be needed, or not needed:

Parameters:

Conditions:

Different KMS Keys based on the Conditions specified above for the type of IAM SVC Users needed. The example includes the DevTeamKMSKey Resource which would be created if the Condition CreateBasicTeam is True (from “No” being selected to pMuleNeeded and pKafkaNeeded). As well as the DevTeamMuleKMSKey Resource which would be created if the Conditon CreateOnlyMule is True (from “Yes” being selected to pMuleNeeded and “No” being selected to pKafkaNeeded):

Hope these example give you some assistance in getting this working,

Brad

Brad Taylor | Data Security Analyst | Information Security | American Century Investments | Brad\_Taylor@americancentury.com | 4500 Main Street | KC, MO 64111

From: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Date: Tuesday, March 3, 2020 at 1:19 PM

To: Brad Taylor <Brad\_Taylor@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>, Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: RE: Cloud Formation

Hi Brad,

I just wondering, if we select READ-ONLY or READ-WRITE. How to make the changes on policy by using single input options. Because policy will change based on the input parameter (READ\_ONLY or READ\_WRITE ).

This above value are referred READ\_ONLY policy. How can I use same policy or common policy for all the Type of access (Could you provide me any suggestion or url or any model template).

Sai

From: Brad Taylor <Brad\_Taylor@americancentury.com>

Sent: Tuesday, March 3, 2020 12:51 PM

To: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>; Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: Re: Cloud Formation

Hey Sai,

So we can actually do the Parameter sections using the MetaData section with a CloudFormation Interface and ParameterGroups. Here is some Docs from AWS on this which may be useful: CloudFormation Interface Docs

This would allow us to have a “Parameter Group” for READ-ONLY, WRITE-ONLY, READ-WRITE, etc. and if the top-level parameter which asks, “Is [TYPE OF ACCESS] needed?” is “No” we would set a Condition to be False for that Access and thereby not create the IAM Data Access Policy for that type of access. Conditions will only equate to “True” when done so in your “Conditions” Section of the CFT if the answer is “Yes”. Therefore, we would then create the IAM Data Access Policy for that type of access as the Condition is met for that Resource to be created.

In CFT we don’t have option to create section for specific parameter. Instead of that, we will use below method to achieve the requirement. Correct me if I am wrong.

pS3BucketType:

Type: String

Description: “Select the type of access. i.e READ-ONLY or READ-WRITE”

Default: “READ-ONLY”

Allowed Values:

- READ-WRITE

- READ-ONLY

- NONE

Not to say that there is anything wrong with the approach you suggested above; however it still limits the CFT to be valid for only type of access at a time, and doesn’t allow it to be used to provision differing types of access via one CFT. This would result in having at minimum 2 CloudFormation Stacks for differing levels of access that is needed, and we have a limit to how many CF Stacks can be in an AWS Account at a time.

Thanks,

Brad

Brad Taylor | Data Security Analyst | Information Security | American Century Investments | Brad\_Taylor@americancentury.com | 4500 Main Street | KC, MO 64111

From: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Date: Monday, March 2, 2020 at 2:48 PM

To: Brad Taylor <Brad\_Taylor@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>, Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: RE: Cloud Formation

Hi Brad,

I made some changes in CFT and attached in email chain.

I need to understand some more about below point.

In CFT we don’t have option to create section for specific parameter. Instead of that, we will use below method to achieve the requirement. Correct me if I am wrong.

pS3BucketType:

Type: String

Description: “Select the type of access. i.e READ-ONLY or READ-WRITE”

Default: “READ-ONLY”

Allowed Values:

- READ-WRITE

- READ-ONLY

- NONE

Also, What we need to do, if the user selects “None” while on starting section template. Based on that, we need to write the template.

Thank You,

Sai

From: Brad Taylor <Brad\_Taylor@americancentury.com>

Sent: Friday, February 28, 2020 6:55 AM

To: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>; Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: Re: Cloud Formation

My apologies, I forgot to include the example of the mappings and Roles: functionality in an IAM Policy. I’ve modified the info inline to my original email.

Brad Taylor | Data Security Analyst | Information Security | American Century Investments | Brad\_Taylor@americancentury.com | 4500 Main Street | KC, MO 64111

From: Brad Taylor <Brad\_Taylor@americancentury.com>

Date: Friday, February 28, 2020 at 6:47 AM

To: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>, Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: Re: Cloud Formation

Good Morning Sai,

I have made a few modifications to your CFT you sent over to help with some complexities that explaining in an email would be difficult! 😊

In short my changes are:

• Moved around some of the Parameter Groups, and changed descriptions

• Added a new Parameter “pS3BucketPath” to fit a little neater with the Resources section. You had the “pS3Path” as the Bucket Resource, which would have caused problems with access

• Added a new Parameter “pS3BucketName” for the same reason as above

• Modified the “pAWSRequestNumber” Parameter with the info you requested

• Modified the “pTeamName” Parameter with the info you requested

• Modified the Descriptions on each Policy to reflect the Team it is for in the Description (just my nitpickiness, nothing wrong with the way you had it)

• Modified the Resources on each Policy to reflect the new S3 Bucket Parameters

It looks great so far, and good progress.

Here is I think our next steps for a complete and working CFT which we can begin to deploy:

• In the IAM Policy use the “Roles:” functionality to attach the IAM Policy to the actual Team who is requesting access so that the Permissions are added without any manual steps.

o Here is an example of how you might do so:

Addition of the new Mapping, “ACITeamName”, which maps the Team Name from the Parameters to the IAM Access Role for the Team

In the IAM Policy addition of something like this section for the “Roles:” functionality to attach this new IAM Policy to an IAM Role:

Finally for our MVP3, I think we will want to try to achieve some of these items:

• As I had mentioned in my previous email, make the S3 Bucket Name (pS3BucketName) and S3 Bucket Path (pS3BucketPath) a list which can then be split out and then access to multiple S3 Buckets and/or Paths can be done at once. This would allow us to add/remove Access as needed, without the need to create a new IAM Policy with new access, or manually update the IAM Policy once the initial skeleton created in this CFT is done.

• Addition of a Parameter Group for S3 Paths for READ-ONLY, READ-WRITE, etc. and have a simple Parameter at the beginning of the section asking if any access of that type is needed, and if it is to complete the section accordingly. If not, user can continue to next section. Still allows you to retain the Conditions you have, but makes the CFT more generic and modular instead of siloed for each type of access as a different Stack.

o Ex.

 READ-ONLY Access Section

• pS3ReadOnlyBucketNames

• pS3ReadOnlyBucketNameAndPaths

Thanks,

Brad

Brad Taylor | Data Security Analyst | Information Security | American Century Investments | Brad\_Taylor@americancentury.com | 4500 Main Street | KC, MO 64111

From: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Date: Thursday, February 27, 2020 at 10:30 AM

To: Brad Taylor <Brad\_Taylor@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>, Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: RE: Cloud Formation

Good Morning Brad,

As per the email, I have modified CloudFormation Template. Please take a look(Attached file).

 Modified the parameter name with prefix “p”

 Modified the S3 bucket name with path (ps3Path)

 Added one more parameter filed with AWS requested filed

 Rearranged the S3 bucket type

I need some inputs to complete the CFT. Can you provide the below information.

 Required list of Team-Name (to update in CFT)

 Required List of S3bucketname with Path

 AWS Request Numbers ( Is it AWS account number or any other ?)

Thank You,

Sai

From: Brad Taylor <Brad\_Taylor@americancentury.com>

Sent: Wednesday, February 26, 2020 7:51 AM

To: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>; Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: Re: Cloud Formation

Sai,

So far so good! There are a couple of things we need to change:

• Addition of the Parameter for S3 Bucket Path

o This can either be part of the “pS3Bucket” Parameter and change it’s name to “pS3Path” or a new Parameter, but you will need to be sure to match the Bucket Name and Bucket Path accordingly in your CFT.

o The reason being that we do not grant access at the root of the Bucket and all Objects as there are different hierarchies of access.

 Ex.

• Each S3 Bucket and appropriate access is separated at the highest level (Data Domain), and access is that level instead the root. These would look like the following:

o [S3 BUCKET]/investment – this is all Investment Data which does not have specific license/access requirements

o [S3 BUCKET]/client – this is all Client Data

• Parameters should always be pre-fixed with a lowercase “p” to signify that it is a Parameter.

o The reason is that Resource Names will not have any “pre-fix” so it can easily be confused what is being Referenced in the “!Ref” function.

o Ex.

 Parameter “S3Bucket” would be “pS3Bucket”

 Parameter “TeamName” would be “pTeamName”

• Addition of the Parameter for AWS Request Number

o This allows us to track when/how Access was granted and which Request it was made a part of.

o I think this would work best as a List of Strings. Then when a new Data Access Request is received, we can add it to the list of Requests to track the lineage of Access Requests.

o Should be added to the Description for each IAM Managed Policy, joining to the description of the Policy.

 As an example the Description would look like this:

• Potentially you could bring this into sections, whereby there is a Parameter Group for S3 Paths for READ-ONLY, READ-WRITE, etc. and have a simple Parameter at the beginning of the section asking if any access of that type is needed, and if it is to complete the section accordingly. If not, user can continue to next section. Still allows you to retain the Conditions you have, but makes the CFT more generic and modular instead of siloed for each type of access as a different Stack.

Good progress so far, and I look forward to the next iteration!

Thanks,

Brad

Brad Taylor | Data Security Analyst | Information Security | American Century Investments | Brad\_Taylor@americancentury.com | 4500 Main Street | KC, MO 64111

From: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Date: Wednesday, February 26, 2020 at 7:26 AM

To: Brad Taylor <Brad\_Taylor@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>, Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: RE: Cloud Formation

Hi Brad,

Thanks for giving me the idea to start work on CFT.

As I created a demo template where you can see and correct me.

Below are the parameters of demo CFT.

Attached a copy in email chain and to meet your requirement I’m more open to make changes in CFT

Thank You,

Sai

From: Brad Taylor <Brad\_Taylor@americancentury.com>

Sent: Monday, February 24, 2020 8:44 AM

To: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>; Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: Re: Cloud Formation

Hey Sai,

So Chris and I are interested in getting our S3 Bucket Access Provisioning automated, or as close to automated as we can on the IAM side.

At a high-level as we reviewed Friday, the goal would be to do the following:

• Create a CFT which would use this information to automate provisioning of the access via an IAM Policy (noting still that the S3 Bucket Policies will need to be updated to reflect the same permissions)

o Create an IAM Policy for the specified Team which dynamically adds/removes the access needed based on the information in the Request

o When a new Data Access Request is received:

 Run an update on the CFT where you add the name & path to the list of S3 Buckets and Paths

• This would then retain the old Buckets and folder access while adding the new ones to the IAM Policy dynamically

o When a Request to remove access, or delete an S3 Bucket is received:

 Do the same as above, but it would remove the ones which are no longer in the list of S3 Buckets and Paths

Here would be the known parameters in the CFT:

o Team Name

 STRING - Drop-down as we have on the same template I sent over to you

o S3 Bucket Name(s) & Folder Path(s)/Subdirectory(s) which permissions need added

 LIST of STRINGS – List of the S3 Buckets and the respective paths

• Ex: aci-dl-bronze-dev-48-us-east-2/client/\*

o Level of access for the Requested S3 Buckets and respective paths

 STRING – Drop-down selection

• Ex: READ-ONLY

Given the Approved Request, we would know the following information and can populate the CFT appropriately:

o Team Name

o S3 Bucket Name(s)

o Folder Path(s)/Subdirectory(s) which permissions need added

o Level of access for the Request

 READ-ONLY

 READ-WRITE

 READ-WRITE-DELETE

 WRITE-DELETE

We can certainly sit down and review this in more detail if you’d like?

Thanks,

Brad

Brad Taylor | Data Security Analyst | Information Security | American Century Investments | Brad\_Taylor@americancentury.com | 4500 Main Street | KC, MO 64111

From: Saiteja Tadepu <Saiteja\_Tadepu@americancentury.com>

Date: Monday, February 24, 2020 at 8:17 AM

To: Brad Taylor <Brad\_Taylor@americancentury.com>

Cc: Bryon McKee <Bryon\_McKee@americancentury.com>, Chris Hartley <Chris\_Hartley@americancentury.com>

Subject: Cloud Formation

Hi Brad,

Could you please confirm me what exactly do I need to work on CloudFormation.

Please give me detailed resources to take a charge on CFT.

I have reviewed the template which you provided me last Friday but not sure where I can help you with it.

Thank You,

Sai