Grand Central User's Guide :

Version 1.0

08/30/2019

Author : Kamilo “Kam” Amir

Table of Contents

Getting Started

Amazon Web Services

Requirements

Grand Central works with the AWS Organizations framework and does not require either Landing Zone or Control Tower to work. By having the organization setup with multiple accounts, Grand Central will be able to discover the accounts and add into management within Splunk.

Please refer to the Amazon Web Services documentation on how to get started with Organizations :
https://aws.amazon.com/premiumsupport/knowledge-center/get-started-organizations/

Before Deploying Grand Central

You will need to be able to create an IAM User in the Master Account and the sub accounts that will be added into management under Splunk. By default there will be two IAM policies created, one to list all the accounts in the Organization and the second will be a deployment policy.

Setting up your Grand Central Environment

You will need to create an IAM User in your master account that has a policy with access to list organizations. Here is an example of the JSON Policy :

IAM Policy - Grand_Central_Lister_Policy

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "organizations:ListAccounts",
         "Resource": "*"
      }
   ]
}
```

Next, each AWS Account will need to have the following IAM User and Policy created in order to deploy the data collection capabilities for Splunk :

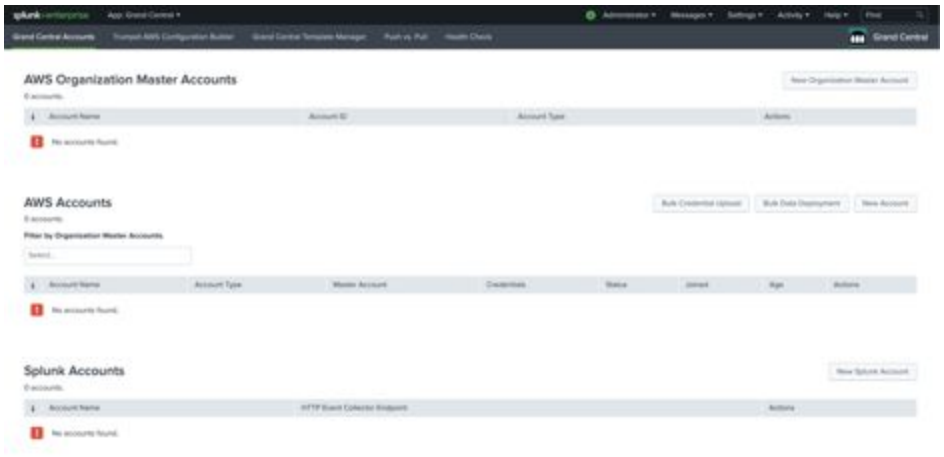
IAM Policy - `Grand_Central_Deployer_Policy` :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "iam:GetAccountPasswordPolicy",
                "kinesis:Get*",
                "iam:CreateRole",
                "s3:CreateBucket",
                "iam:AttachRolePolicy",
                "lambda:GetFunctionConfiguration",
                "iam:PutRolePolicy",
                "kinesis:ListStreams",
                "s3:GetObjectAcl",
                "iam:DetachRolePolicy",
                "logs:GetLogEvents",
                "events:RemoveTargets",
                "lambda:DeleteFunction",
                "events:PutEvents",
                "s3:GetBucketPolicyStatus",
                "iam:GetRole",
                "events:DescribeRule",
                "lambda:InvokeFunction",
                "iam:GetAccessKeyLastUsed",
                "firehose:CreateDeliveryStream",
                "cloudformation:*",
                "iam:DeleteRole",
                "firehose:DescribeDeliveryStream",
                "s3:GetObject",
                "sts:AssumeRole",
                "logs:PutSubscriptionFilter",
                "s3:GetLifecycleConfiguration",
                "s3:GetBucketTagging",
                "logs:DescribeLogStreams",
                "events:PutRule",
                "s3:GetBucketLogging",
                "s3:ListBucket",
                "s3:GetAccelerateConfiguration",
                "iam:CreateUser",
                "s3:GetBucketPolicy",
                "firehose:DeleteDeliveryStream",
                "iam:PassRole",
                "sns:Get*",
                "sns:Publish",
                "iam:DeleteRolePolicy",
                "s3:DeleteBucket",
                "s3:PutBucketVersioning",
                "iam:ListAccessKeys",
                "s3:GetBucketPublicAccessBlock",
                "logs:DescribeLogGroups",
                "kinesis:DescribeStream",
                "iam:DeleteUser",
                "sns:List*",
                "events:PutTargets",
                "events:DeleteRule",
                "lambda:AddPermission",
                "s3:ListAllMyBuckets",
                "s3:GetBucketCORS",
                "iam:ListUsers",
                "iam:GetUser",
                "s3:GetBucketLocation",
                "lambda:RemovePermission"
            ],
            "Resource": "*"
        }
    ]
}
```

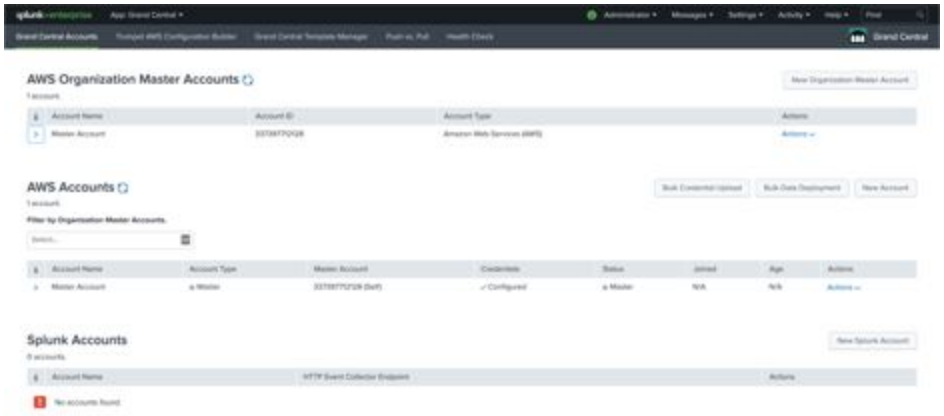
Download the credentials files into a single directory for all the accounts. Once you have all the files (e.g. credentials.csv, credentials-1.csv) then run the credentials_consolidator.py which will create all_account_credentials.json.

Adding Master Account

Log into the Grand Central App and navigate to the Accounts Section.



Click on the “New Organization Master Account” button:



The Master Account will now be added to your console:

AWS Account Setup

* Account ID: 337397712128

The AWS Account ID of this account.

* Account Name: Master Account

A descriptive name for the account and any applied CloudFormation stacks. A name can contain only alphanumeric characters (case-sensitive) and hyphens.

* Account Type: Amazon Web Services (AWS)

The public cloud service this account is from

* AWS Access Key: AKIAU5DTYQUAONIMZ7VP

An AWS Access Key for this account with appropriate permissions attached

* AWS Secret Key: ••

An AWS Secret Key for this account with appropriate permissions attached

Add or remove tags

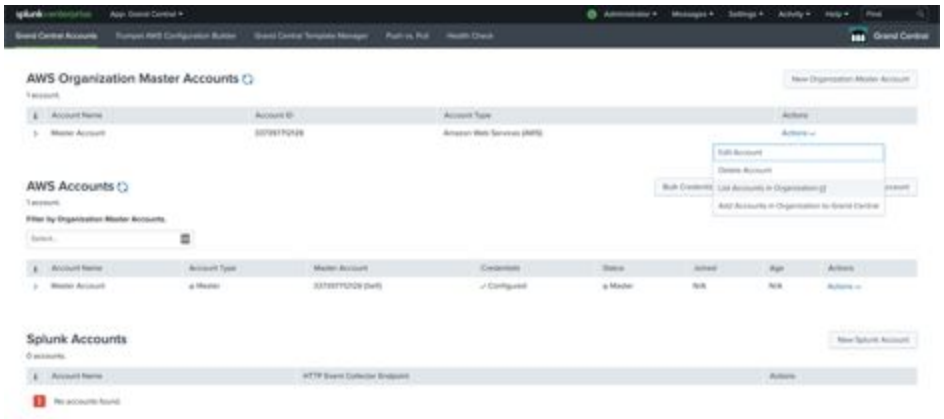
MasterAccount

+ Add Row

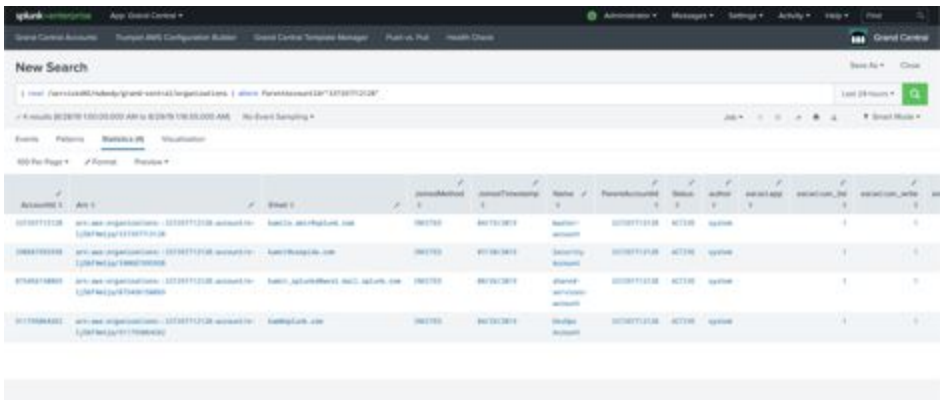
* Indicates required field.

Cancel | Save

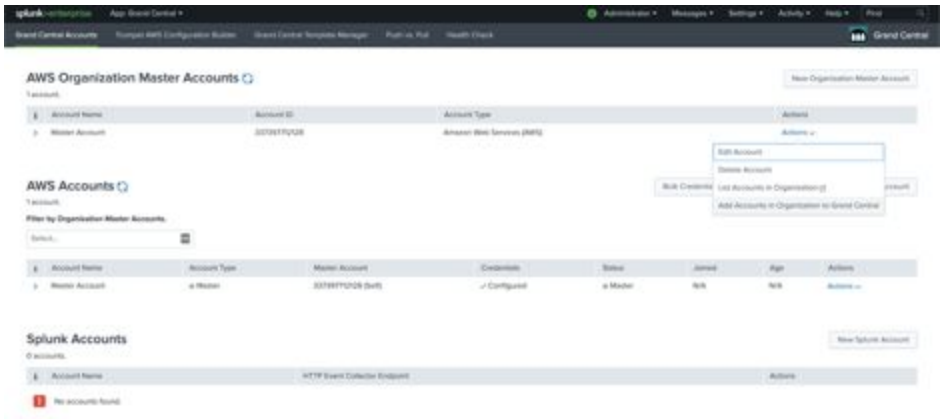
Next, validate this IAM user has access to list all the accounts in the organization:



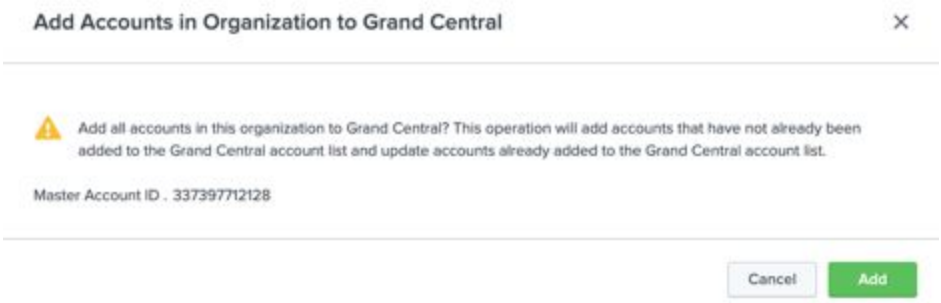
All the available accounts should show up in a Splunk Search window:



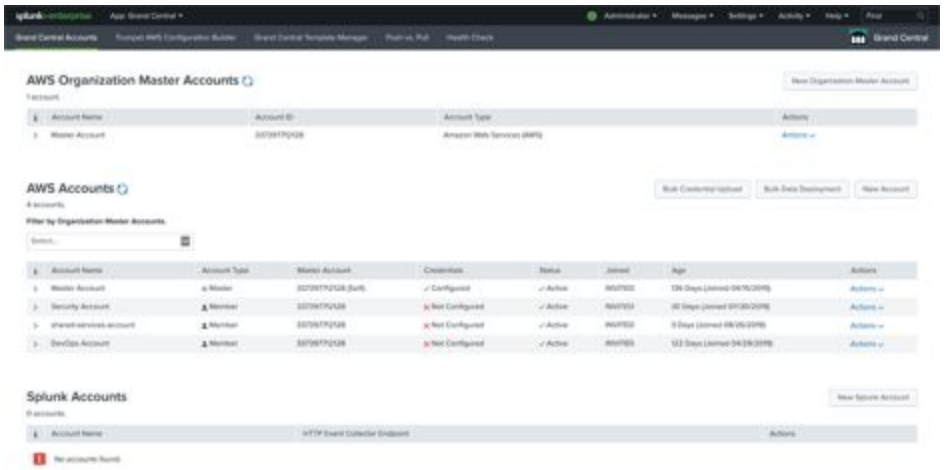
Now add the accounts into management:



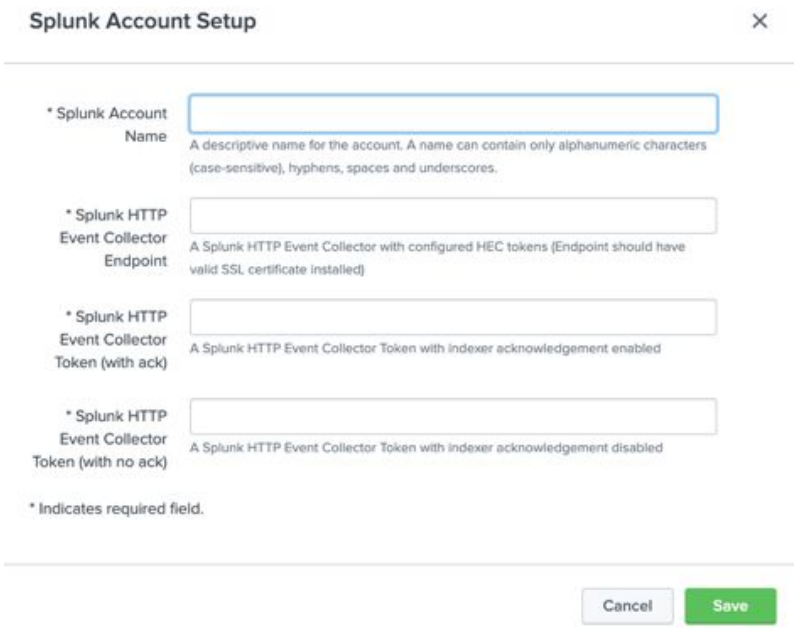
Click the Add button:



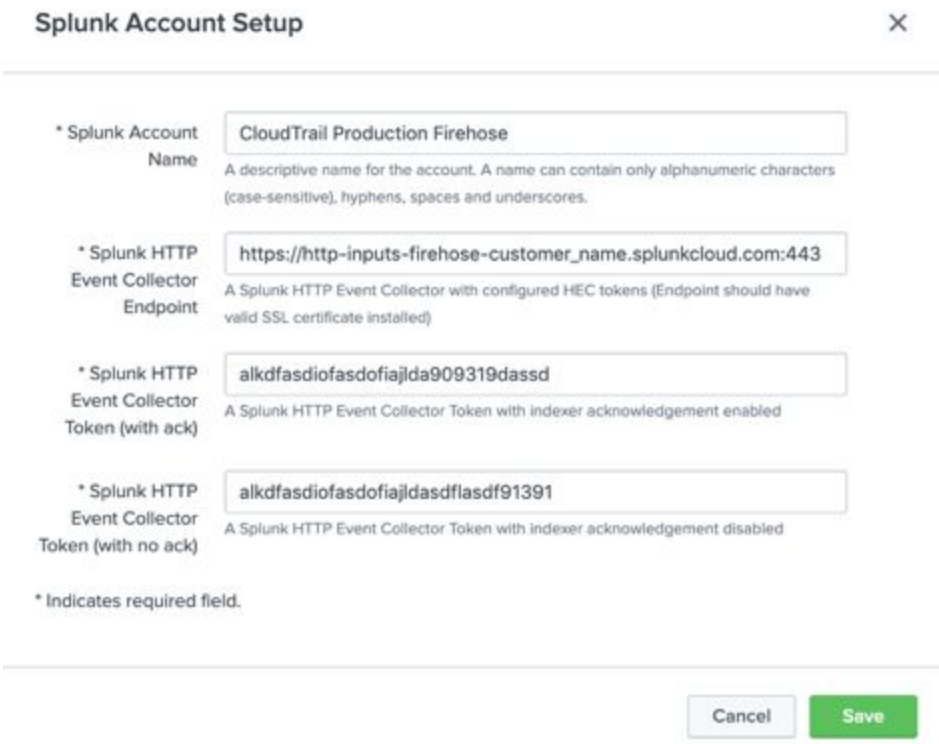
All the accounts in your organization will now show up in Splunk :



Now, add the destination where you will be sending your data. This is typically a Firehose endpoint on your Splunk Cloud Deployment.



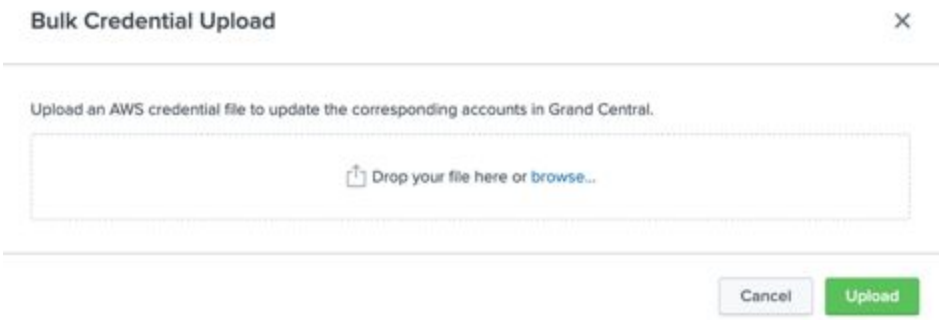
Here is an example of how you should fill out the fields:



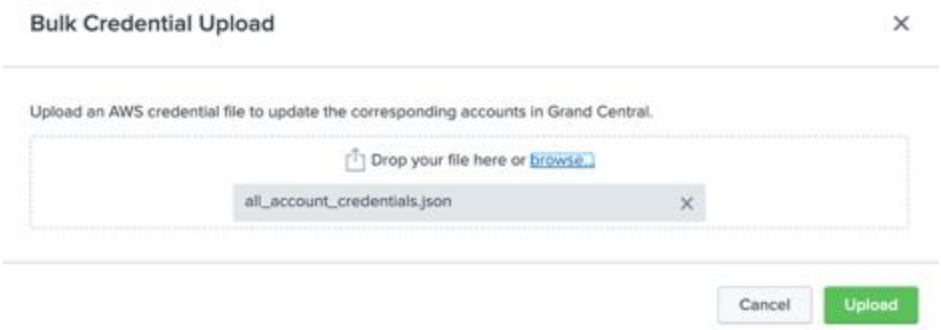
Note that if you are using Splunk Cloud the URL for your firehose endpoint should look like this: https://http-inputs-firehose-<customer_name>.splunkcloud.com:443

Where <customer_name> is your stack name. The port (:443) needs to be put in the URL in order for this system to work.

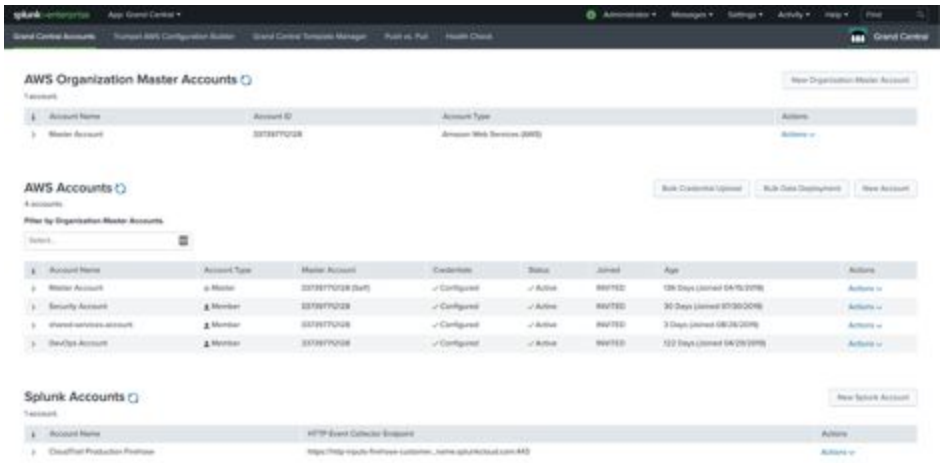
Now let's bulk upload your credentials file (all_accounts.json) that you created from all your credential.csv files:



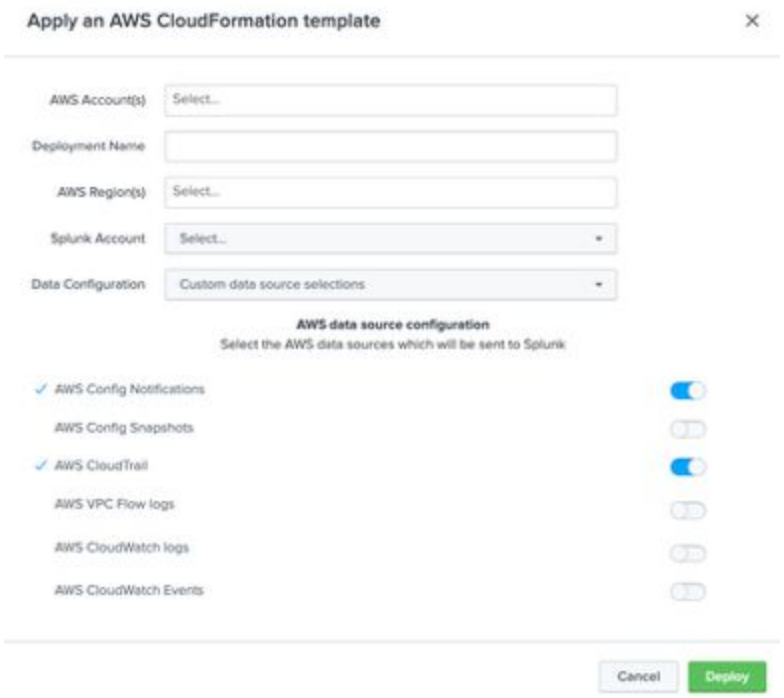
Upload your file:



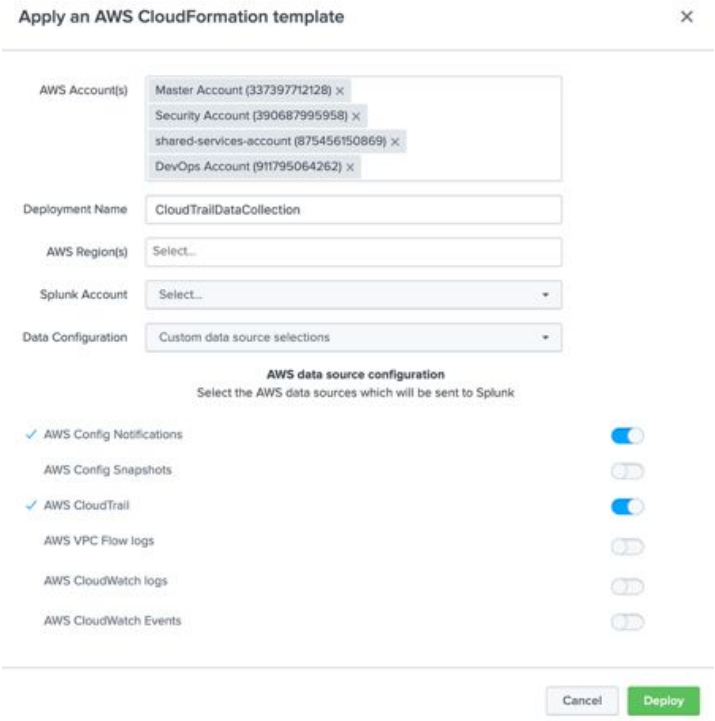
Now, all your accounts should have their credentials added to your Splunk Deployment:



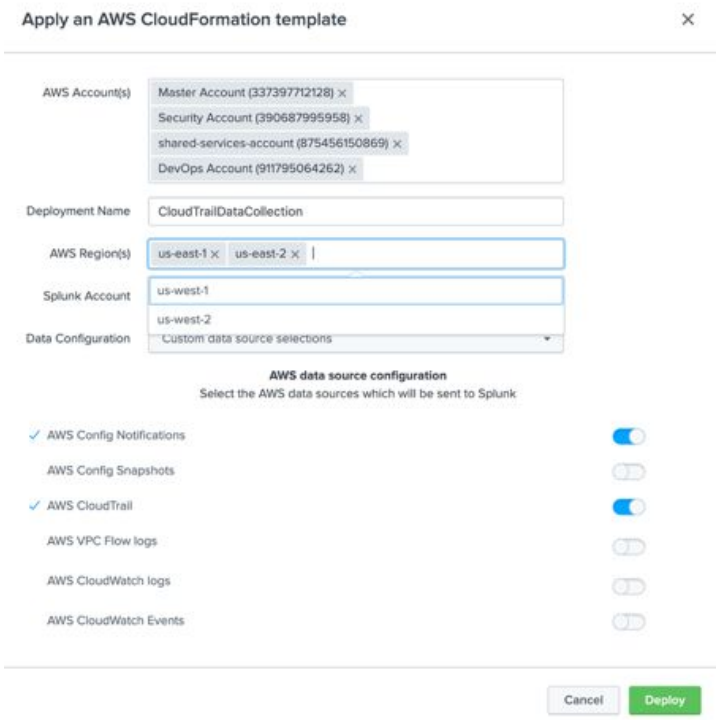
Finally, now let's deploy data collection to all these accounts:



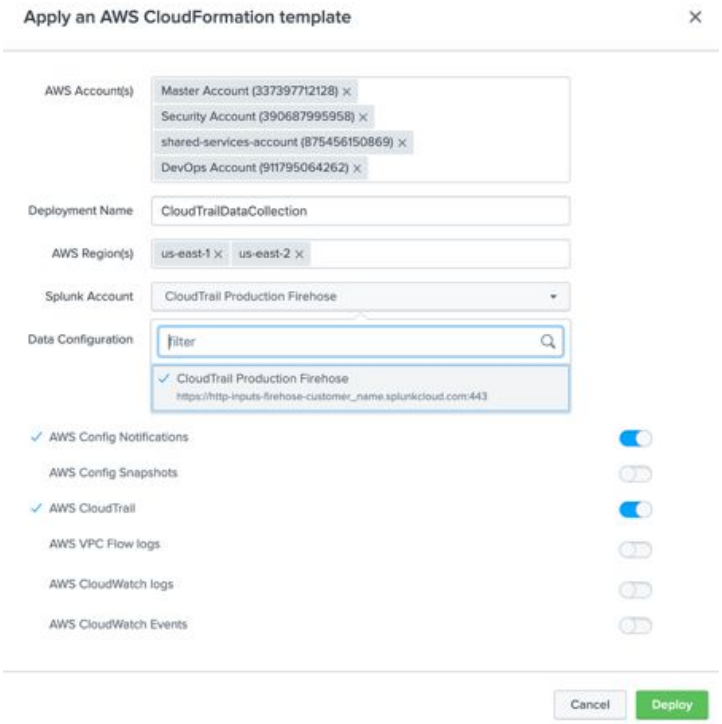
Select the accounts you want to deploy data collection templates to:



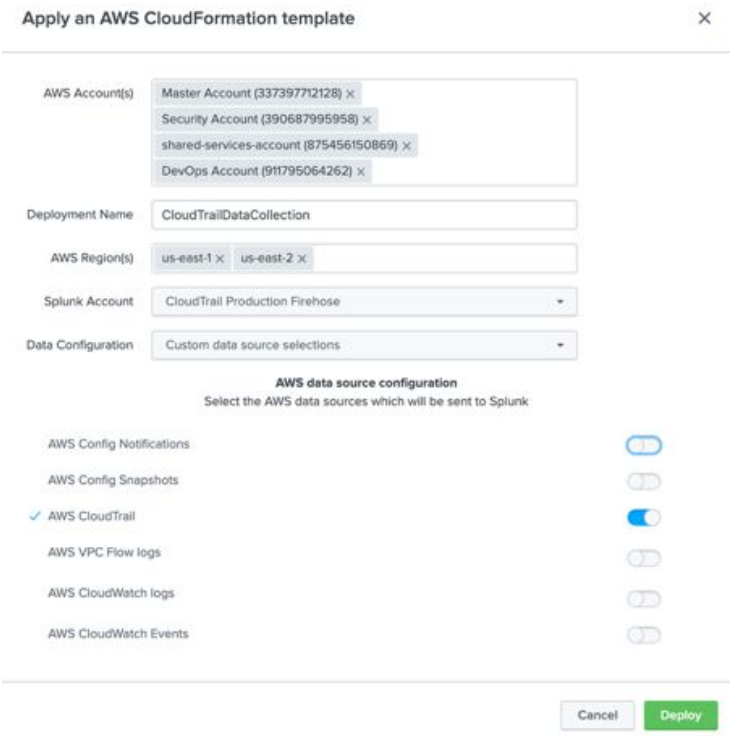
Select the regions:



Then the destination (Splunk Account):



Select the AWS data source(s) you want to send into Splunk and click Deploy



Google Cloud Platform

TBD

Azure

TBD