

Grand Central User's Guide :

Version 1.1.1

01/30/2020

Author : Kamilo "Kam" Amir

Table of Contents

Getting Started	3
Amazon Web Services	3
Requirements	3
Before Deploying Grand Central	4
Setting up your Grand Central Environment	5
Adding Master Account	7
Google Cloud Platform	8
Azure	8

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": [
        "autoscaling:Describe*",
        "cloudformation:*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricData",
        "config:DeliverConfigSnapshot",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:GetComplianceDetailsByConfigRule",
        "config:GetComplianceSummaryByConfigRule",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "events:DescribeRule",
        "events:PutEvents",
        "events:PutRule",
        "events:PutTargets",
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteUser",
        "iam:DetachRolePolicy",
        "iam:GetAccessKeyLastUsed",
        "iam:GetAccountPasswordPolicy",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListAccessKeys",
        "iam:ListUsers",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "kinesis:DescribeStream",
        "kinesis:Get*",
        "kinesis:ListStreams",
        "kms:Decrypt",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:RemovePermission",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
```

```

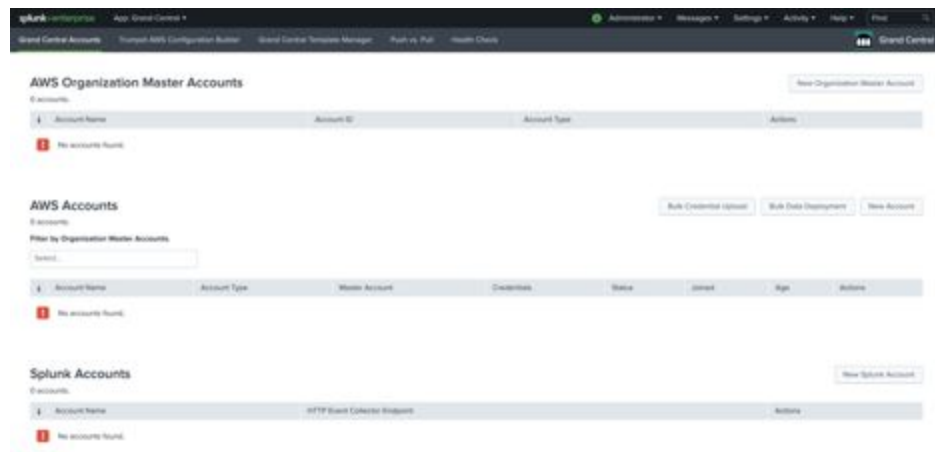
        "s3:GetObjectAcl",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "sns:Get*",
        "sns:List*",
        "sns:Publish",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sts:AssumeRole"
    ],
    "Resource": "*"
}
]
}
)

```

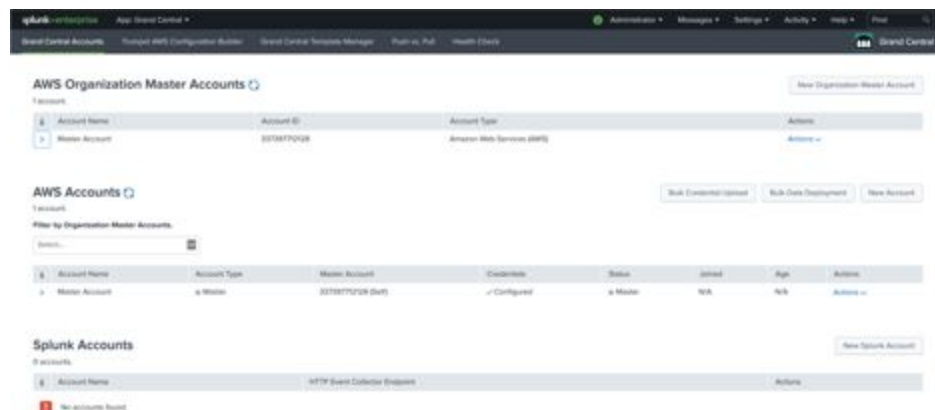
Download the credentials files into a single directory for all the accounts. Once you have all the files (e.g. credentials.csv, credentials-1.csv) then run the credentials_consolidator.py which will create all_account_credentials.json.

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

X

* Account ID

The AWS Account ID of this account.

* Account Name

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

* Account Type

The public cloud service this account is from.

* AWS Access Key

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

X

+ Add Row

* Indicates required field.

Cancel

Save

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

The screenshot shows the Splunk Grand Central interface. At the top, there's a navigation bar with 'Grand Central Accounts', 'Import AWS Configuration Rules', 'Grand Central Template Manager', 'Push to Splunk', and 'Health Check'. The main content area is divided into three sections: 'AWS Organization Master Accounts' (1 account), 'AWS Accounts' (1 account), and 'Splunk Accounts' (0 accounts). The 'AWS Organization Master Accounts' section shows a table with columns: Account Name, Account ID, Account Type, and Actions. The 'AWS Accounts' section shows a table with columns: Account Name, Account Type, Master Account, Credentials, Status, Joined, Age, and Actions. The 'Splunk Accounts' section shows a table with columns: Account Name and Actions. A dropdown menu is open next to the 'Actions' link in the 'AWS Organization Master Accounts' section, showing options: 'Edit Account', 'Delete Account', 'List Accounts in Organization', and 'Add Account to Organization to Grand Central'.

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

The screenshot shows a Splunk Search window. The search bar contains the query: `index=main | eval _source=grandcentral | search | where ParentAccountID="337587712128"`. The search results are displayed in a table with columns: AccountID, Account Name, Account Type, Master Account, Credentials, Status, Joined, Age, and Actions. The table contains four rows of data, each representing an account in the organization.

Now add the accounts into management:

The screenshot shows the Splunk Grand Central interface, identical to the first screenshot. It displays the 'AWS Organization Master Accounts', 'AWS Accounts', and 'Splunk Accounts' sections. The 'AWS Organization Master Accounts' section shows a table with columns: Account Name, Account ID, Account Type, and Actions. The 'AWS Accounts' section shows a table with columns: Account Name, Account Type, Master Account, Credentials, Status, Joined, Age, and Actions. The 'Splunk Accounts' section shows a table with columns: Account Name and Actions. A dropdown menu is open next to the 'Actions' link in the 'AWS Organization Master Accounts' section, showing options: 'Edit Account', 'Delete Account', 'List Accounts in Organization', and 'Add Account to Organization to Grand Central'.

Click the **Add** button:

Add Accounts in Organization to Grand Central

Add all accounts in this organization to Grand Central? This operation will add accounts that have not already been added to the Grand Central account list and update accounts already added to the Grand Central account list.

Master Account ID . 337397712128

Cancel

Add

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

[Splunk](#)
[App Store Center](#)

[Administration](#)
[Messages](#)
[Settings](#)
[Activity](#)
[Help](#)
[Feedback](#)

[Brand Central Accounts](#)
[Inspect AWS Configuration Builder](#)
[Brand Central Template Manager](#)
[Push vs. Pull](#)
[Health Check](#)

AWS Organization Master Accounts

1 account

[New Organization Master Account](#)

Account Name	Account ID	Account Type	Actions
Master Account	337587792528	Amazon Web Services (AWS)	Actions

AWS Accounts

4 accounts

[Bulk Customer Onboard](#)
[Bulk Data Onboarding](#)
[New Account](#)

Filter by Organization Master Accounts

Search

Account Name	Account Type	Master Account	Credentials	Status	Joined	Age	Actions
Master Account	Master	337587792528 (Self)	✓ Configured	✓ Active	NA/7582	136 Days (Joined 04/16/2018)	Actions
Security Account	Member	337587792528	✗ Not Configured	✓ Active	NA/7583	30 Days (Joined 07/30/2018)	Actions
aws-elastic-mapreduce-account	Member	337587792528	✗ Not Configured	✓ Active	NA/7585	3 Days (Joined 08/06/2018)	Actions
DevOps Account	Member	337587792528	✗ Not Configured	✓ Active	NA/7585	122 Days (Joined 04/19/2018)	Actions

Splunk Accounts

0 accounts

[New Splunk Account](#)

Account Name	Actions
No accounts found	Actions

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

Splunk Account Setup

X

* Splunk Account Name

A descriptive name for the account. A name can contain only alphanumeric characters (case-sensitive), hyphens, spaces and underscores.

* Splunk HTTP Event Collector Endpoint

A Splunk HTTP Event Collector with configured HEC tokens (Endpoint should have valid SSL certificate installed)

* Splunk HTTP Event Collector Token (with ack)

A Splunk HTTP Event Collector Token with indexer acknowledgement enabled

* Splunk HTTP Event Collector Token (with no ack)

A Splunk HTTP Event Collector Token with indexer acknowledgement disabled

* Indicates required field.

CancelSave

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

Splunk Account Setup

* Splunk Account Name

CloudTrail Production Firehose

A descriptive name for the account. A name can contain only alphanumeric characters (case-sensitive), hyphens, spaces and underscores.

* Splunk HTTP Event Collector Endpoint

https://http-inputs-firehose-customer_name.splunkcloud.com:443

A Splunk HTTP Event Collector with configured HEC tokens (Endpoint should have valid SSL certificate installed)

* Splunk HTTP Event Collector Token (with ack)

alkdfasdiofasdofiajlda909319dassd

A Splunk HTTP Event Collector Token with indexer acknowledgement enabled

* Splunk HTTP Event Collector Token (with no ack)

alkdfasdiofasdofiajldasdfiasdf91391

A Splunk HTTP Event Collector Token with indexer acknowledgement disabled

* Indicates required field.

Cancel

Save

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:

Bulk Credential Upload

Upload an AWS credential file to update the corresponding accounts in Grand Central.

Drop your file here or browse...

Cancel

Upload

Upload your file:

Bulk Credential Upload ✕

Upload an AWS credential file to update the corresponding accounts in Grand Central.

Drop your file here or [browse](#)

all_account_credentials.json ✕

Cancel Upload

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

AWS Organization Master Accounts ✕

New Organization Master Account

Account Name	Account ID	Account Type	Actions
Master Account	337917028	Amazon Web Services (AWS)	Actions ⌵

AWS Accounts ✕

Bulk Credentials Upload

Bulk Data Deployment

New Account

4 accounts

Filter by Organization Master Accounts

Select ⌵

Account Name	Account Type	Master Account	Credentials	Status	Joined	Age	Actions
Master Account	Master	337917028 (Self)	✓ Configured	✓ Active	8/17/20	136 Days (Joined 04/16/2019)	Actions ⌵
Security Account	Member	337917028	✓ Configured	✓ Active	8/17/20	30 Days (Joined 07/30/2019)	Actions ⌵
Shared-services-account	Member	337917028	✓ Configured	✓ Active	8/17/20	3 Days (Joined 08/26/2019)	Actions ⌵
DevOps Account	Member	337917028	✓ Configured	✓ Active	8/17/20	122 Days (Joined 04/29/2019)	Actions ⌵

Splunk Accounts ✕

New Splunk Account

Account Name	HTTP Event Collector Endpoint	Actions
CloudTrail Production Pipeline	https://http-inputs- <i>Production</i> - <i>name</i> .splunkcloud.com/443	Actions ⌵

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

Apply an AWS CloudFormation template ✕

AWS Account(s) Select...

Deployment Name

AWS Region(s) Select...

Splunk Account Select...

Data Configuration Custom data source selections

AWS data source configuration

Select the AWS data sources which will be sent to Splunk

✓ AWS Config Notifications ☒

AWS Config Snapshots ☐

✓ AWS CloudTrail ☒

AWS VPC Flow logs ☐

AWS CloudWatch logs ☐

AWS CloudWatch Events ☐

Cancel Deploy

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

Apply an AWS CloudFormation template

AWS Account(s)

Master Account (337397712128) x
Security Account (390687995958) x
shared-services-account (875456150869) x
DevOps Account (911795064262) x

Deployment Name

CloudTrailDataCollection

AWS Region(s)

Select...

Splunk Account

Select...

Data Configuration

Custom data source selections

AWS data source configuration

Select the AWS data sources which will be sent to Splunk

✓ AWS Config Notifications

AWS Config Snapshots

✓ AWS CloudTrail

AWS VPC Flow logs

AWS CloudWatch logs

AWS CloudWatch Events

Cancel

Deploy

Select the regions:

Apply an AWS CloudFormation template

AWS Account(s)

Master Account (337397712128) x
Security Account (390687995958) x
shared-services-account (875456150869) x
DevOps Account (911795064262) x

Deployment Name

CloudTrailDataCollection

AWS Region(s)

us-east-1 x us-east-2 x |

Splunk Account

us-west-1

Data Configuration

us-west-2
Custom data source selections

AWS data source configuration

Select the AWS data sources which will be sent to Splunk

✓ AWS Config Notifications

AWS Config Snapshots

✓ AWS CloudTrail

AWS VPC Flow logs

AWS CloudWatch logs

AWS CloudWatch Events

Cancel

Deploy

Then the destination (Splunk Account):

Apply an AWS CloudFormation template

AWS Account(s)

Master Account (337397712128) x
Security Account (390687995958) x
shared-services-account (875456150869) x
DevOps Account (911795064262) x

Deployment Name

CloudTrailDataCollection

AWS Region(s)

us-east-1 x us-east-2 x

Splunk Account

CloudTrail Production Firehose

Data Configuration

filter

CloudTrail Production Firehose
https://http-inputs-firehose-customer_name.splunkcloud.com/443

✓ AWS Config Notifications

AWS Config Snapshots

✓ AWS CloudTrail

AWS VPC Flow logs

AWS CloudWatch logs

AWS CloudWatch Events

Cancel

Deploy

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

Apply an AWS CloudFormation template

AWS Account(s)

Master Account (337397712128) x
Security Account (390687995958) x
shared-services-account (875456150869) x
DevOps Account (911795064262) x

Deployment Name

CloudTrailDataCollection

AWS Region(s)

us-east-1 x us-east-2 x

Splunk Account

CloudTrail Production Firehose

Data Configuration

Custom data source selections

AWS data source configuration
Select the AWS data sources which will be sent to Splunk

✓ AWS CloudTrail

AWS Config Notifications

AWS Config Snapshots

AWS VPC Flow logs

AWS CloudWatch logs

AWS CloudWatch Events

Cancel

Deploy

Google Cloud Platform

TBD

Azure

TBD