Implementation Guide:

Splunk Grand Central Integration for Control Tower
# Table of Contents

Foreword .................................................................................................................. 4
Solution overview and features ...................................................................................... 5
Architecture diagram ..................................................................................................... 5
Pre-requisites ................................................................................................................ 6
Splunk Deployment ....................................................................................................... 7
  Splunk Cloud .............................................................................................................. 7
  Splunk Bring Your Own License (BYOL) .................................................................. 7
Deployment Steps ......................................................................................................... 7
  Prepare your Master Account ..................................................................................... 7
  IAM User and Policy ................................................................................................. 7
  Prepare your Splunk Deployment ............................................................................. 8
Install Grand Central .................................................................................................... 8
Configure Grand Central for AWS Organizations / Control Tower ............................ 8
  Setup AWS Master Account .................................................................................... 8
  Setup Splunk (HEC) Endpoints .............................................................................. 10
  Discover and Add AWS Accounts .......................................................................... 13
Create Stack Set .......................................................................................................... 14
Deploy Data Collection ............................................................................................... 16
  Bulk Credential Upload (optional if not using StackSets) ...................................... 17
  Bulk Data Deployment (optional if not using StackSets) ....................................... 18
FAQ ............................................................................................................................ 20
  CloudFormation Deployment ................................................................................... 20
  Kinesis Data Firehose ............................................................................................... 20
  Troubleshooting HEC (CLI) .................................................................................... 20
  Troubleshooting HEC (Web/UI) ............................................................................. 20
Additional resources .................................................................................................... 21
Best Practices .................................................................................................................. 23

- Use valid SSL Certificates for your Splunk deployment. If using Firehose, make sure that you have indexer ACK enabled on your Splunk deployment ................................................................. 23
- When in doubt, please refer to the Splunk ....................................................................... 23

Solution Estimated Pricing .................................................................................................. 23
Partner contact information .................................................................................................. 23
Foreword

The Splunk integration for AWS Control Tower is a solution that enables customers to manage and gain visibility to their AWS Organization at scale. This integration comes in the form of the Splunk App Grand Central and has a direct integration into the AWS Organization and AWS Control Tower services.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Splunk in AWS Control Tower environment while taking full advantage of the resources pre-configures by AWS Control Tower as part of the initialization.
Solution overview and features

Splunk is the Data-to-Everything Platform that allows you to bring data to every question, decision and action. The Grand Central App allows you to integrate into your AWS Organization and instantly gain visibility across all of your accounts. This solution allows you to rapidly collect all the data from your accounts and send them serverlessly into Splunk via HTTP Event Collector (HEC).

All of this is done by leveraging StackSets and trusts between your Primary Account and your AWS Accounts. AWS Control Tower can be used to deploy the initial account setup and then Splunk can be used to detect drift and automatically report and correct the drifted account. Both newly vended accounts and existing accounts can be configured by Splunk using Grand Central.

With Splunk, you can:

- Gain instant visibility on your AWS Organization
- Deploy data collection to new and existing AWS Accounts
- Detect drift from guardrails and other configuration rules
- Centralize visualization of logs, metrics and applications
- Maintain continuous data collection from your entire AWS Organization

Architecture diagram

This solution requires that you deploy an AWS Identity and Access Management (IAM) Policy, Role and account from your primary account. Splunk leverages AWS CloudFormation templates, AWS Lambda functions, Amazon Simple Storage Service (Amazon S3) buckets and Amazon CloudWatch Events to enable these features.

Figure 1 Grand Central Splunk App Workflow Architecture Diagram
Pre-requisites

For enhanced capabilities, enabling AWS Control Tower would help with creating clearly defined Guardrails for your AWS Deployment. Clearly defined Organizational Units (OU) will help properly deploy templates for data collection. Administrator access to the Master Account will also be required in order to create the required IAM Policy, Role and other AWS Artifacts. Finally, the administrator must enable the Prerequisites for Stack Set Operations.

This solution functions as described only in commercial AWS Regions. This solution has limitations in GovCloud. Splunk is working on a solution for our GovCloud customers.

Prior to deploying this solution, make sure to get approval from your Security and Operations teams so that you do not modify or impair any of your existing accounts. Validate that the IAM Policy, Roles, and users are approved prior to deployment.

Map out how your accounts will be linked to Organizational Units (OU) and that you have prior approval to deploy those changes to the accounts. This Account to OU mapping will be critical for how Splunk deploys templates into each AWS Account.

Users must have some working knowledge of Amazon Web Services (AWS), specifically around AWS Identity and Access Management (IAM), AWS CloudFormation Templates, StackSets, AWS Lambda Functions, Amazon CloudWatch, and Amazon Simple Storage Service (Amazon S3) buckets. Splunk knowledge will also be required in order to properly configure the integration with AWS and AWS Control Tower. If you are new to AWS, see Getting Started with AWS: https://aws.amazon.com/getting-started/.


To get started with AWS Control Tower, check out the https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html
Splunk Deployment

Make sure you are running Splunk version 7.2+ and that you have Grand Central installed on your search head. This system must have access to the internet as it will be making REST calls into AWS to launch CloudFormation templates. The Splunk user should have Power User at minimum to use Grand Central.

Splunk Cloud

Customers can request Splunk Cloud on the AWS Marketplace or contact Splunk directly.

Splunk Bring Your Own License (BYOL)

Splunk can also be deployed using the AWS Marketplace AMI that is running version 7.2 or better.

Amazon Kinesis Data Firehose must be able to access the Splunk HTTP Event Collector (HEC) and requires the endpoint to be a publicly facing URL with a valid SSL Certificate (not self-signed). The Data Input associated with the HEC must have Indexer Acknowledgment turned ON. Splunk Cloud customers can use the URL http-inputs-firehose-<custom_URL>.-splunkcloud.com. Please see all the requirements for Kinesis Data Firehose here.

Deployment Steps

Prepare your Master Account

Make sure your AWS team is familiar with the StackSets Concepts prior to deploying this solution. Once they have understood what will be happening in your AWS Master Account, please enable Trusted Access with AWS Organizations. This will require administrator privileges in the Master Account.

IAM User and Policy

The Master account will require an IAM user with a policy that will allow for it to deploy stack sets to the child accounts in your Organization. There are two primary IAM Policies that should be called out; first the GrandCentral Master policy is used for the Master Account to setup the data collection and the trust for the stacksets. Control Tower / AWS Organization Enabled Policy (StackSet Policy):

This policy can be automatically deployed in your Master Account by running this CloudFormation Template found here:


Individual Accounts / AWS Organization Policy (Optional Single Account Policy):
This second IAM Policy is optional and can be used to setup each account to setup and collect data sources.

This policy can be automatically deployed in your Master Account by running this CloudFormation Template found here:

Prepare your Splunk Deployment

Your Splunk Deployment should have an HEC endpoint accessible to your AWS Deployment and follow the guidelines for enabling a Kinesis Data Firehose input.

Install Grand Central

Install the Grand Central App from the Splunkbase.

Configure Grand Central for AWS Organizations / Control Tower

Setup AWS Master Account

In your AWS Console, get the Access Key / Secret Key for the Grand Central List Account. This can be found in the CloudFormation Outputs tab:
AWS Account Setup

* Account ID
12345678
The AWS Account ID of this account.

* Account Name
PrimaryAccount
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
AAAAAAAAAAAAAAAAAAAA
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

* Indicates required field.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account ID</td>
<td>AWS Account ID (must be the account number)</td>
</tr>
<tr>
<td>Account Name</td>
<td>Descriptive name of the account. It can contain alphanumeric characters and hyphens</td>
</tr>
<tr>
<td>Account Type</td>
<td>Cloud Provider (AWS)</td>
</tr>
<tr>
<td>AWS Access Key</td>
<td>Access key for IAM User</td>
</tr>
<tr>
<td>AWS Secret Key</td>
<td>Secret key for IAM User</td>
</tr>
<tr>
<td>Tags</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Setup Splunk (HEC) Endpoints

Splunk HTTP Event Collector (HEC) endpoints are URL’s with the associated tokens to collect data into Splunk without the need of a Heavy Forwarder.

### Splunk Account Setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Account Name (required)</td>
<td>Name of your Splunk Endpoint, an example would be CloudTrailEndpoint.</td>
</tr>
<tr>
<td>Splunk HTTP Event Collector (HEC) Endpoint</td>
<td>This is the FQDN of your Splunk HEC Endpoint. An example would be <a href="https://http-inputs-firehose-mystack.splunkcloud.com:443">https://http-inputs-firehose-mystack.splunkcloud.com:443</a> <em>The port is required</em></td>
</tr>
<tr>
<td>Splunk HEC with ACK</td>
<td>Endpoints that have Indexer ACK enabled (e.g. Firehose enabled HEC).</td>
</tr>
<tr>
<td>Splunk HEC with no ACK</td>
<td>Endpoints with no indexer ACK enabled (e.g. Lambda functions or other HEC resources).</td>
</tr>
</tbody>
</table>
Pro Tips:

- If your endpoint only has one HEC Token, just put the token in twice.
- Please note that you need the :443 or :8088 (depending on your deployment) at the end of the URL in order for this to work properly.

For Splunk Cloud customers, your URL will look like this:

http-inputs-firehose-my-stack.splunkcloud.com:443

- Note, replace ‘my-stack’ with the name of your Splunk Cloud Stack.
- The port, ‘:443’ is required for Firehose to properly send the data into Splunk Cloud.

For Splunk BYOL or Self-Managed Instances, your URL may vary and the port might be 8088:

splunk.yourdomain.com:8088

- Note, replace ‘splunk.yourdomain.com’ with the name of your Splunk Deployment.
- The port, ‘:8088’ is required for Firehose to properly send the data into Splunk Cloud. Your port may be different, please check with your Splunk administrators and make sure you allow that port through your Security Groups.
Example Form Filled Out:

### Splunk Account Setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Splunk Account Name</td>
<td>CloudTrail</td>
</tr>
<tr>
<td>* Splunk HTTP Event Collector Endpoint</td>
<td><a href="https://http-inputs-firehose-mystack.splunkcloud.com:443">https://http-inputs-firehose-mystack.splunkcloud.com:443</a></td>
</tr>
<tr>
<td>* Splunk HTTP Event Collector Token (with ack)</td>
<td>AAAAAAAAAAAAA123123123123123123</td>
</tr>
<tr>
<td>* Splunk HTTP Event Collector Token (with no ack)</td>
<td>AAAAAAAAAAAAA123123123123123123</td>
</tr>
</tbody>
</table>

* Indicates required field.
Discover and Add AWS Accounts

Click on Grand Central Accounts under AWS and select the action menu. Validate you have the proper credentials and click on List AWS Accounts. This will open a Splunk search window with all of your AWS accounts in your organization.

After you verified your permissions, click on Add Accounts in Organization to Grand Central.
Create Stack Set

Click on New Stackset:

Select your Organization Master Account and the OU that will be tied to the template deployments:

Deploy a AWS Stackset

- AWS Organization Master Account
- AWS Organization Unit
- Deployment Name
- AWS Region(s)
- Splunk Account
- Data Configuration

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

[Deploy]
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Organization Master Account</td>
<td>Your AWS Master IAM Account</td>
</tr>
<tr>
<td>AWS Organization Unit</td>
<td>OU’s tied to deploying CloudFormation Templates</td>
</tr>
<tr>
<td>Deployment Name</td>
<td>Stackset Name</td>
</tr>
<tr>
<td>AWS Region(s)</td>
<td>Geographic data center regions</td>
</tr>
<tr>
<td>Splunk Account</td>
<td>Splunk HEC endpoint</td>
</tr>
<tr>
<td>Data Configuration (optional)</td>
<td>Use to deploy custom templates</td>
</tr>
<tr>
<td><strong>AWS Data source configuration</strong></td>
<td></td>
</tr>
<tr>
<td>AWS Config Notifications</td>
<td>Notifications from AWS Config service</td>
</tr>
<tr>
<td>AWS Config Snapshots</td>
<td>Config Snapshots</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>CloudTrail events</td>
</tr>
<tr>
<td>AWS VPC Flow logs</td>
<td>VPC Flow logs from CloudWatch logs</td>
</tr>
<tr>
<td>AWS CloudWatch logs</td>
<td>Custom CloudWatch Logs</td>
</tr>
<tr>
<td>AWS CloudWatch Events</td>
<td>Custom CloudWatch Events</td>
</tr>
</tbody>
</table>
Deploy Data Collection

Organization Admins can invoke Splunk by moving accounts into specific OU’s based on how the Stacksets were configured. For example, if all of your existing AWS Accounts in your Organization are in the “Development” OU and you move them to “Production” then you can have Splunk automatically deploy the CloudFormation template that will configure “CloudTrail, Config, Amazon Macie, Amazon GuardDuty” and send that data into Splunk via HEC.

![Splunk Integration into Control Tower / Account Vending](image-url)
Bulk Credential Upload (optional if not using StackSets)

Create a JSON file with following format to include your AWS credentials:

```json
{
    "credentials": [
        {
            "category": "1",
            "key_id": "AAAAAAAAAAAAAAAAAAA",
            "secret_key": "AaBbCcDdEeFfGgHhIiJjKkLmMnNn12345678901",
            "name": "SplunkUser-Account1"
        },
        {
            "category": "1",
            "key_id": "AAAAAAAAAAAAAAAAAAA",
            "secret_key": "AaBbCcDdEeFfGgHhIiJjKkLmMnNn12345678901",
            "name": "SplunkUser-Account2"
        },
        {
            "category": "1",
            "key_id": "AAAAAAAAAAAAAAAAAAA",
            "secret_key": "AaBbCcDdEeFfGgHhIiJjKkLmMnNn12345678901",
            "name": "SplunkUser-Account3"
        },
        {
            "category": "1",
            "key_id": "AAAAAAAAAAAAAAAAAAA",
            "secret_key": "AaBbCcDdEeFfGgHhIiJjKkLmMnNn12345678901",
            "name": "SplunkUser-Accountn"
        }
    ]
}
```

Upload the file to your Grand Central App by the Bulk Credentials Upload button:

*AWS Organization Master Accounts*

- **Account Name**: 
- **Account ID**: 
- **Account Type**: 
- **Actions**

<table>
<thead>
<tr>
<th>i</th>
<th>Account Name</th>
<th>Account ID</th>
<th>Account Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No accounts found.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*AWS Accounts* 

- **Bulk Credential Upload**
- **Bulk Data Deployment**
- **New Account**

Upload the file:
If the accounts already exist from your Organization, Splunk will automatically add their credentials. If you do not have an Organization or the credential file contains accounts not in your Organization, they will show up as “Individual” accounts under Account Type.
Organization with separate individual accounts:

Bulk Data Deployment (optional if not using StackSets)

Now you can deploy CloudFormation templates to all the accounts listed under management in Grand Central:
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Accounts</td>
<td>Select all the AWS Accounts you want to deploy the CloudFormation templates into</td>
</tr>
<tr>
<td>Deployment Name</td>
<td>Name of your Stack deployment. If you are using the IAM Policy templates provided in this guide, your deployment name <strong>MUST</strong> start with grandcentral (e.g. grandcentralCloudTrail)</td>
</tr>
<tr>
<td>AWS Region(s)</td>
<td>Geographic data center regions</td>
</tr>
<tr>
<td>Splunk Account</td>
<td>Splunk HEC endpoint</td>
</tr>
<tr>
<td>Data Collection (optional)</td>
<td>Used if you have custom templates you want to deploy</td>
</tr>
</tbody>
</table>

**AWS Data source configuration**

| AWS Config Notifications     | Notifications from AWS Config service                                |
| AWS Config Snapshots         | Config Snapshots                                                     |
| AWS CloudTrail              | CloudTrail events                                                    |
| AWS VPC Flow logs           | VPCFlow logs from CloudWatch logs                                    |
| AWS CloudWatch logs         | Custom CloudWatch Logs                                               |
| AWS CloudWatch Events       | Custom CloudWatch Events                                             |
FAQ:

CloudFormation Deployment

Permission issues tend to be the leading cause of issues with this deployment. Make sure your Master IAM user has the proper policy applied and permission to the resources in the account. If you run into an error see the “Events” tab in the CloudFormation stack to see what is causing the error. Typically, it’s a missing IAM Policy that prevents the stack from being created.

Kinesis Data Firehose

You will need to make sure that your Kinesis Data Firehose endpoint is available to the internet with a valid SSL cert. Follow the steps to troubleshoot Splunk Destination:https://docs.aws.amazon.com/firehose/latest/dev/troubleshooting.html#data-not-delivered-to-splunk

Troubleshooting HEC (CLI)

In Splunk Cloud, test to see if your HEC URL resolves to an IP of a Load Balancer:

bash %: nslookup http-inputs-firehose-stack_id.splunkcloud.com

bash % nslookup http-inputs-firehose-stack_id.splunkcloud.com

Server: 10.160.20.4
Address: 10.160.20.4#53

Non-authoritative answer:


Name: stack_id-hec-ack-444444.us-east-1.elb.amazonaws.com
Address: 1.1.1.1

Name: stack_id-hec-ack-444444.us-east-1.elb.amazonaws.com
Address: 2.2.2.2

Name: stack_id-hec-ack-444444.us-east-1.elb.amazonaws.com
Address: 3.3.3.3

Troubleshooting HEC (Web/UI)

Next, in a browser make sure the hostname and health port resolve and are healthy:

https://http-inputs-firehose-<stack_id>.splunkcloud.com:443/services/collector/health/1.0

Response : {"text":"HEC is healthy","code":17}

Replace <stack_id> with your stack’s name.
Additional resources:

AWS Stackset Administration:

Kinesis Data Firehose:
https://docs.splunk.com/Documentation/AddOns/released/Firehose/ConfigureFirehose
https://docs.aws.amazon.com/firehose/latest/dev/troubleshooting.html#data-not-delivered-to-splunk

Developer License for Splunk:

Download Splunk from https://www.splunk.com or use the AMI from the Marketplace.
Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2020</td>
<td>Initial publication</td>
<td>•</td>
</tr>
</tbody>
</table>

© 2020, Amazon Web Services, Inc. or its affiliates, and Splunk, Inc. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.
Best Practices

- Make sure to use SAML based authentication when logging into your Splunk deployment. Enable two factor authentication for added security.
- Use valid SSL Certificates for your Splunk deployment. If using Firehose, make sure that you have indexer ACK enabled on your Splunk deployment.
- When in doubt, please refer to the Splunk documentation.

Solution Estimated Pricing

This solution will not increase your existing costs since the services and data being collected is already enabled in your accounts. For an estimate in your Splunk license, please contact your sales team and they can help with your questions.

Partner contact information

Please contact sales@splunk.com for any pricing information, partners please use partners@splunk.com and for all support related questions please reach out to support@splunk.com. Our Community (https://community.splunk.com) is a great resource to find answers to your Splunk related questions.