Splunk for AWS

Kam Amir
Matt Poland

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Objective Of This Session

- This session is meant for AWS users who are setting up the Splunk App for AWS (Amazon Web Services).
- We will help you get an understanding of the App and all the AWS components it interacts with.
- This session will also cover troubleshooting the app and properly setting up your AWS environment to work with the App.
- Using the Splunk App for AWS you will gain visibility across your AWS Deployment.

Agenda

- AWS Components
- Permissions for SQS, SNS and S3 buckets
- What's new in Splunk App for AWS v.4.0
- Setting up Splunk App for AWS
- Troubleshooting Splunk App for AWS
- Creating modular inputs for AWS third party apps
- Questions & Answers

AWS Components

splunk>

Terminology

- AWS – Amazon Web Services
  - Amazon's (retailer) Cloud Computing Business
- SQS – Simple Queuing Service
  - Distributed queue messaging service
- SNS – Simple Notification Service
  - Multi-protocol Push notification
- S3 – Simple Storage Service
  - Online file storage service offered by Amazon
  - Provides web services interfaces through SOAP and REST

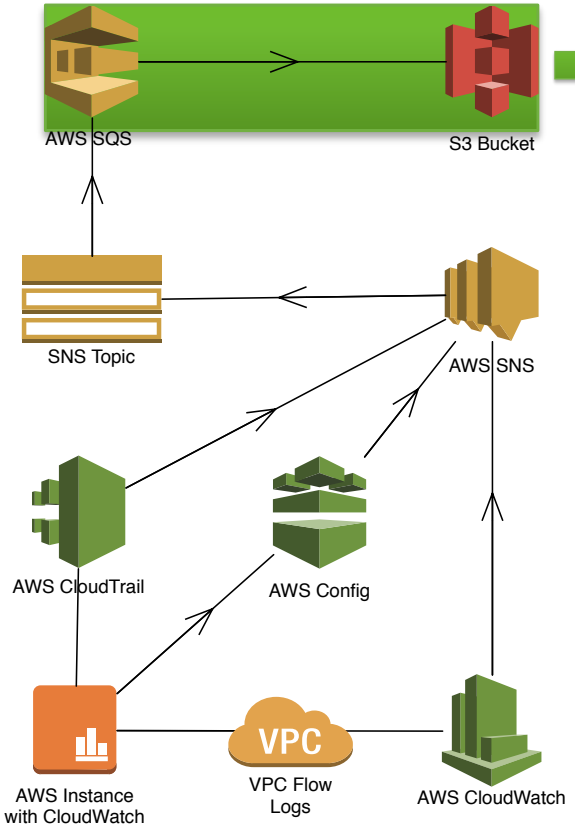
AWS Architecture Diagram

Amazon Storage / Queues

Amazon Messaging

Amazon Logging Layer

Amazon Instances



splunk>cloud
splunk>enterprise

Splunk Collects the data from the AWS SQS and the S3 bucket using the AWS SDK for python (Boto3).

https://aws.amazon.com/sdk-for-python/

Splunk Offerings in AWS

Cloud-service

splunk>cloud

- Splunk Enterprise as a service
- Full app, SDK, API, platform support

splunk>light

- Cloud service designed for small IT environments
- $90 a month

Self-managed

splunk>enterprise

- Self-managed cloud deployments
- Self-deploy in AWS

Hunk

- Integrated with EMR
- Search data in S3
- Hourly pricing

- Splunk App for AWS: Integrates w/CloudTrail, Config and Billing, VPC Flow Logs

Integrations

Splunk App for AWS

- AWS CloudTrail
  - Service that delivers logs of admin activity on AWS infrastructure
  - start/stop/create instance; change user roles/rights; modify network config
  - CloudTrail service simply delivers log files to customers; there is no UI, display, analysis, search etc.
  - **VPC Flow Logs** is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.
- AWS Config
  - AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.
  - With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time.
- AWS Billing

Requirements For Splunk App For AWS

Splunk

- Splunk 6.1 or later
- Splunk Add-on for Amazon Web Services
- Splunk Add-on for Amazon Web Services +1.1.0 required for AWS Config

AWS

- AWS CloudTrail: Enable CloudTrail with SQS and SNS.
- AWS Config: Enable Config with SQS and SNS.
- Billing: Refer to the AWS documentation to turn on AWS detailed billing.
- VPC Flow Logs: Enable VPC Flow log collection.

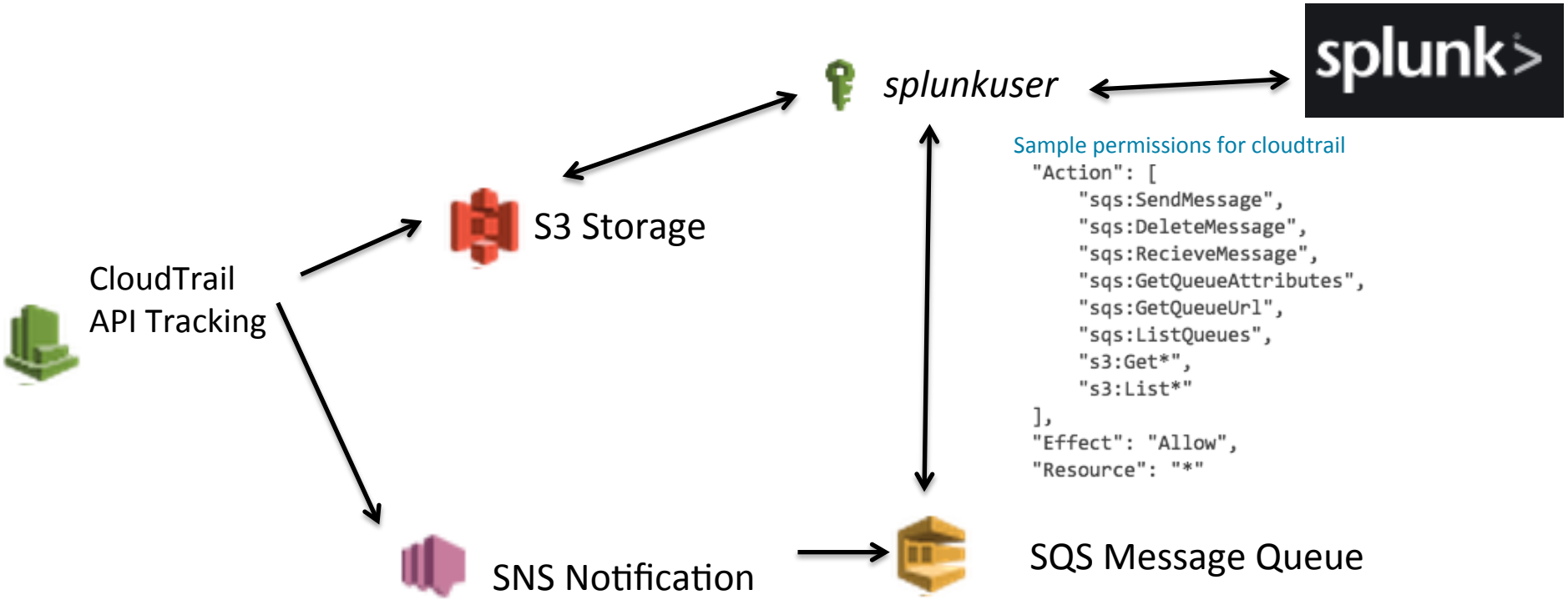
Install the Splunk Add-on for AWS

1. Configure your AWS accounts and services, or confirm your existing configurations.
2. Configure your AWS account permissions to match those required by the add-on.
3. Install the add-on.
4. Set up the add-on on your forwarders or single instance.
5. Configure your inputs to get your AWS data into Splunk Enterprise.

Permissions

splunk>

Permissions



Configure Permissions 1 of 2

- S3 / Billing Permissions

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3:Get*",
    "s3:List*"
   ],
   "Resource": "arn:aws:s3:::*"
  }
 ]
}
```

CloudTrail Permission

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "sqs:GetQueueUrl",
        "sqs:DeleteMessage",
        "s3:Get*",
        "s3:List*"
        "s3:Delete*"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:sqs:*",
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

http://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSpermissions

Configure Permissions 2 of 2

CloudWatch Permission

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": [
    "autoscaling:Describe*",
    "cloudwatch:Describe*",
    "cloudwatch:Get*",
    "cloudwatch:List*",
    "sns:Get*",
    "sns:List*"
   ],
   "Effect": "Allow",
   "Resource": "*"
  }
 ]
}
```

- AWS Config Permission

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "sqs:GetQueueUrl",
        "sqs:DeleteMessage",
        "s3:Get*",
        "s3:List*"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:sqs:*",
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

http://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSpermissions

Splunk App for AWS Setup

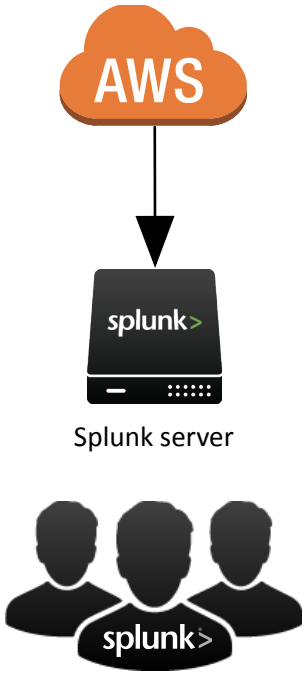
splunk>

Install Add-on for AWS

- Install the Add-on on either a Search Head (Single Deployment) or on a Heavy Weight Forwarder (Distributed Deployment) due to the **Python requirement** and the add-on requires the Splunk Web user interface to perform the **setup and authentication** with AWS.
- The add-on uses the credential vault to secure your credentials, and this credential management solution is **incompatible with the deployment server.**
- The add-on uses modular inputs to collect data remotely. Using a **deployment server** to deploy configured add-ons to multiple forwarders results in **duplicate data collection**.

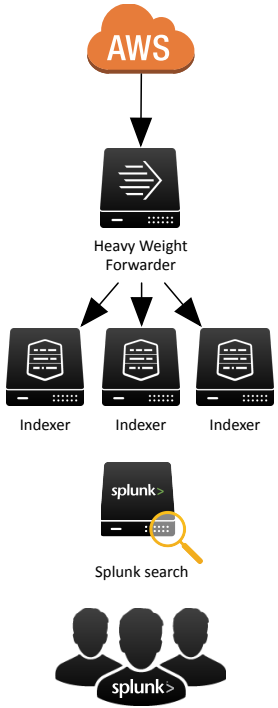
Splunk Architecture

Single Splunk Deployment



Splunk App for AWS installed on all-in-one Splunk server

Distributed Splunk Deployment



Splunk Add-on for AWS installed on Heavy Weight Forwarder

What's New In Splunk App For AWS 4.0

splunk>

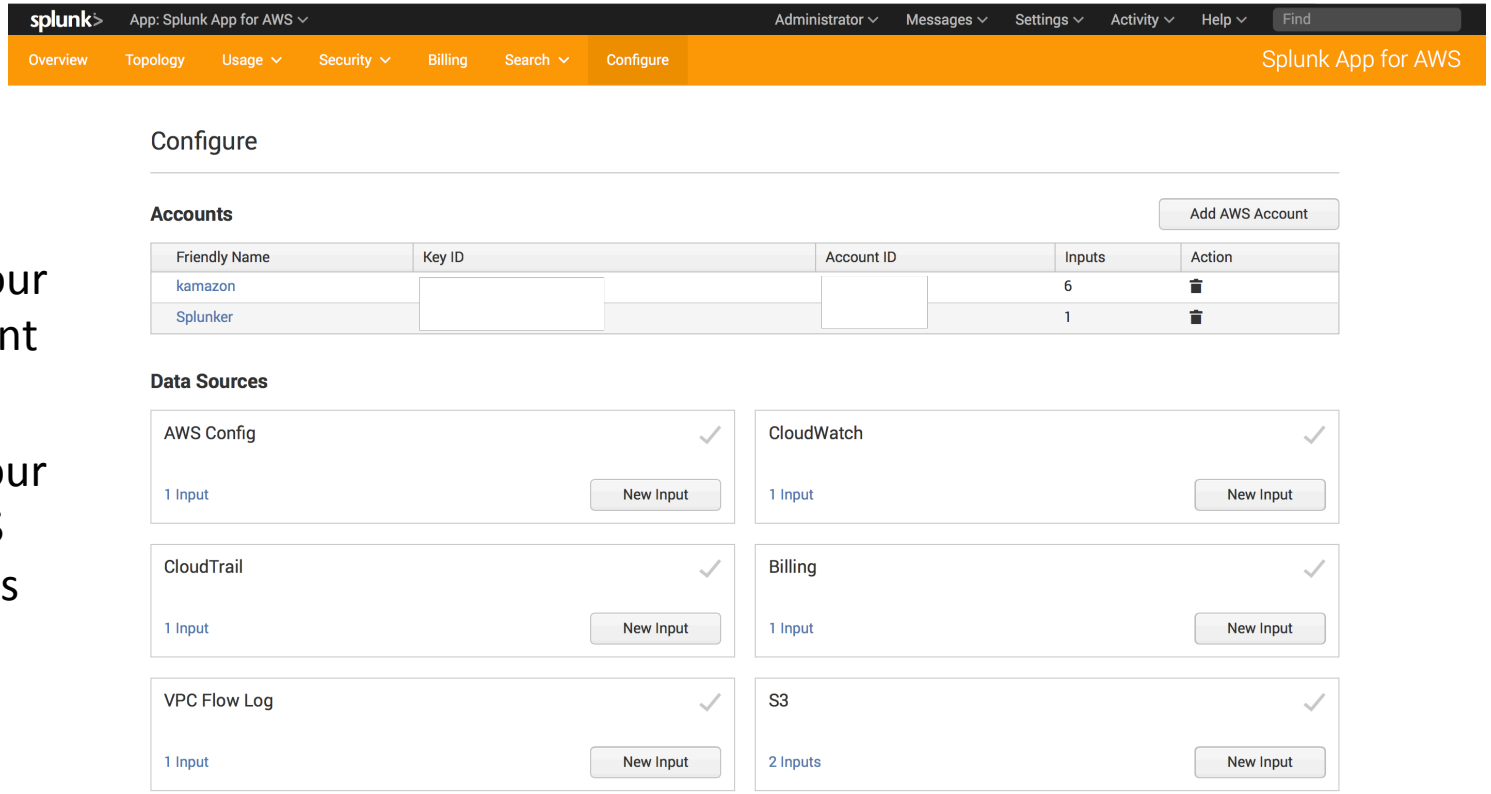
New Features in v.4.0

- Easier onboarding of AWS data
- Enhanced Overview dashboards and reports
- Insight into VPC Flow Data
- Topology View

New Setup 4.0

Add Your Account

Add your AWS Inputs

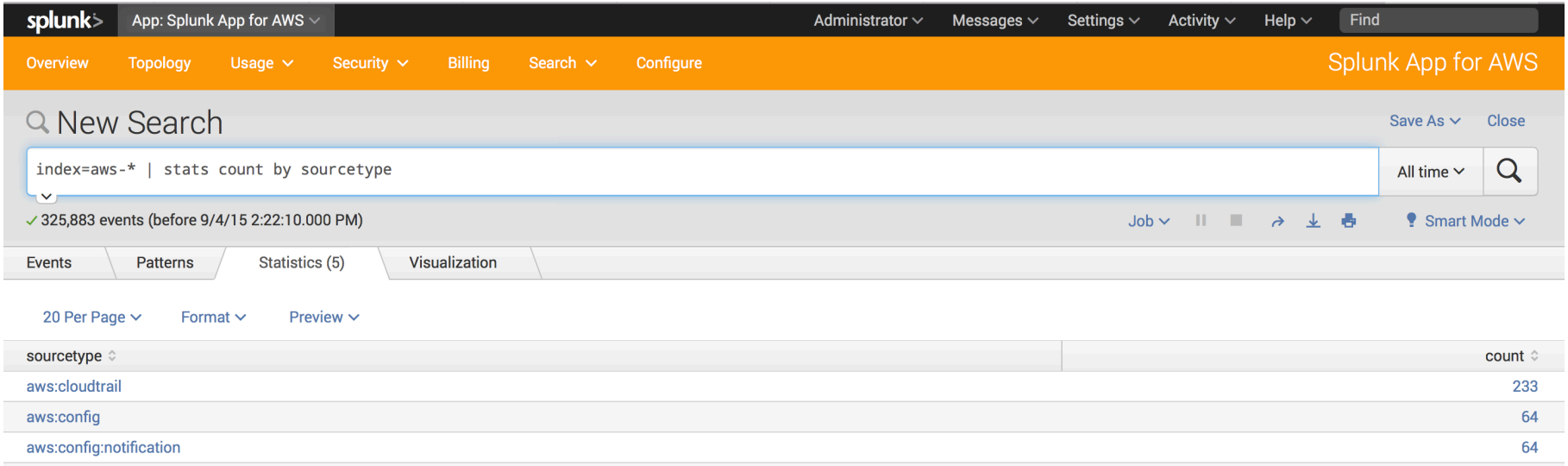


Wait 5 – 10 Minutes

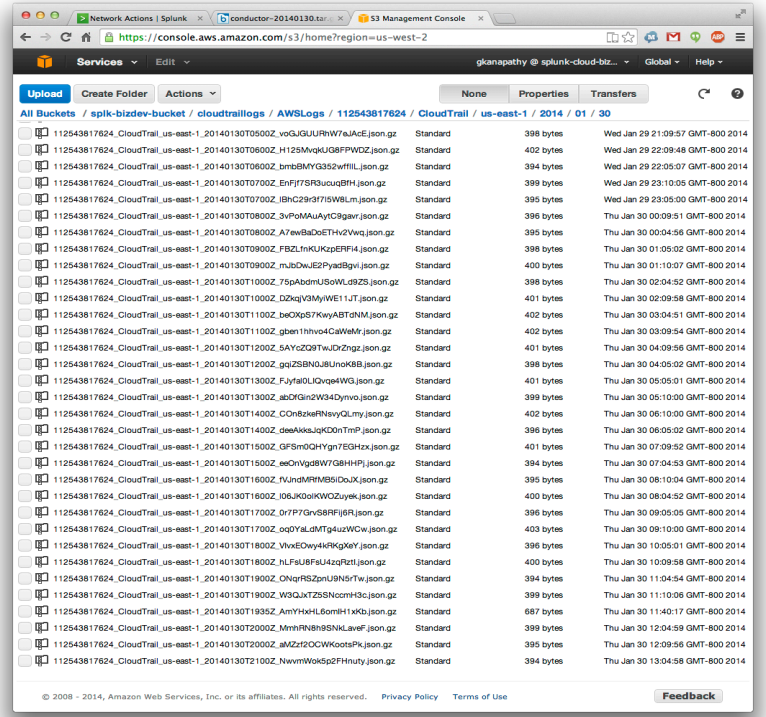
- Yes, you'll need to wait before all the dashboards and reports populate.

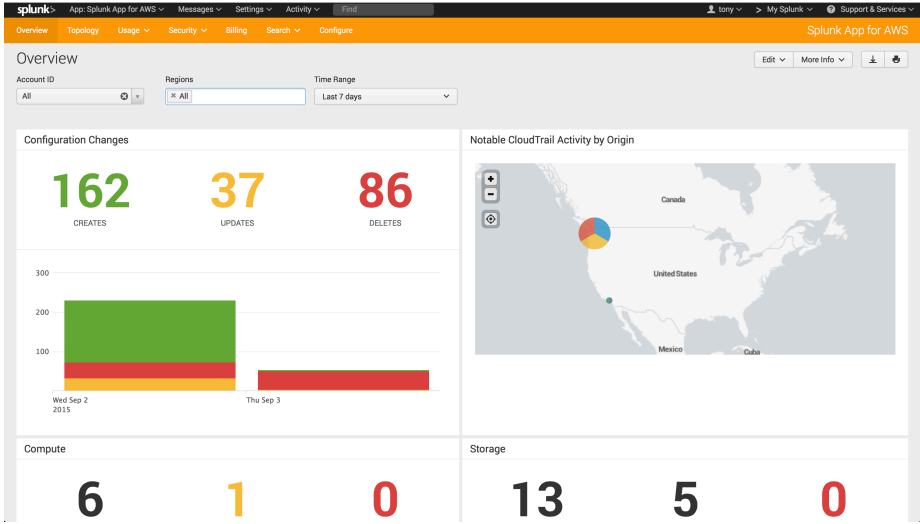
Validate Your Splunk App Setup

- Index=aws-* | stats count by sourcetype

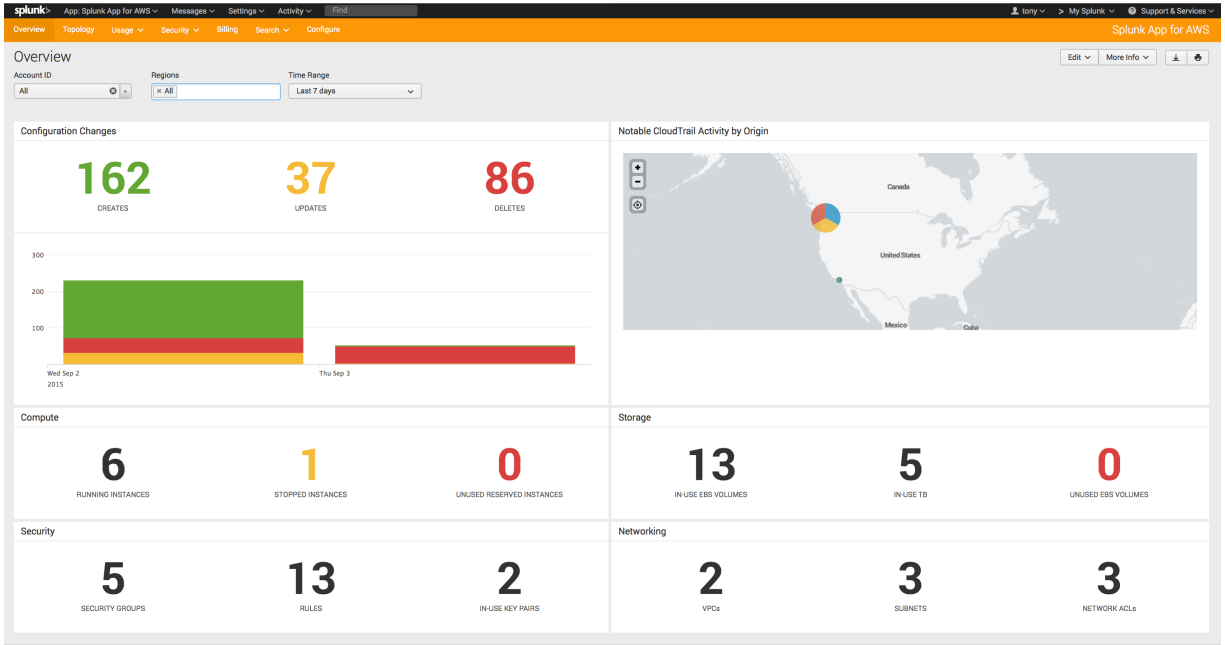


Gain Visibility Into AWS Logs





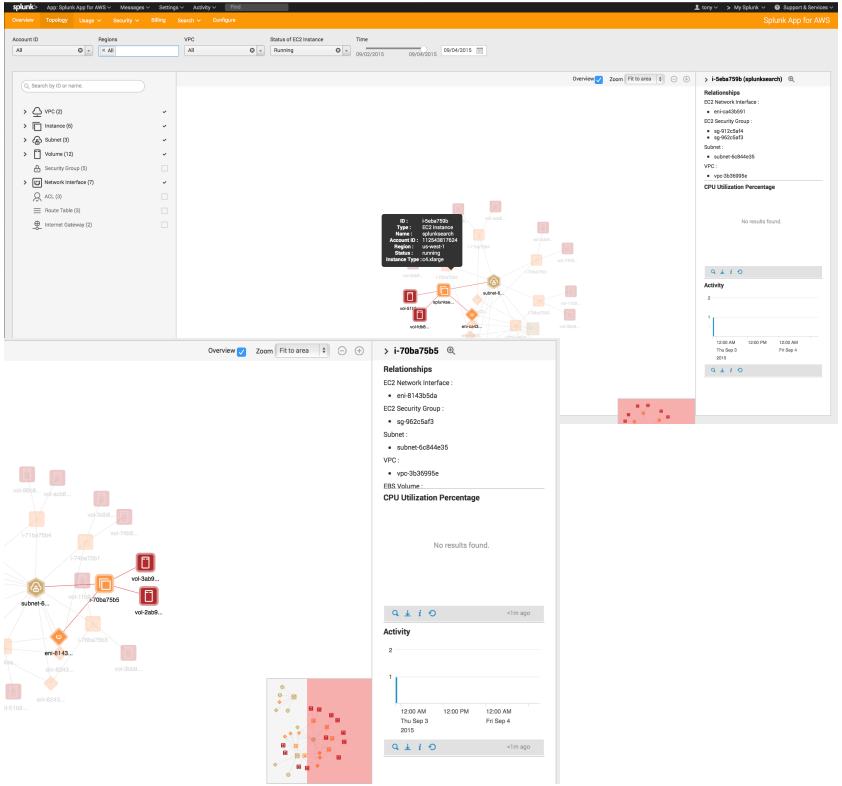
Overview for Splunk App for AWS



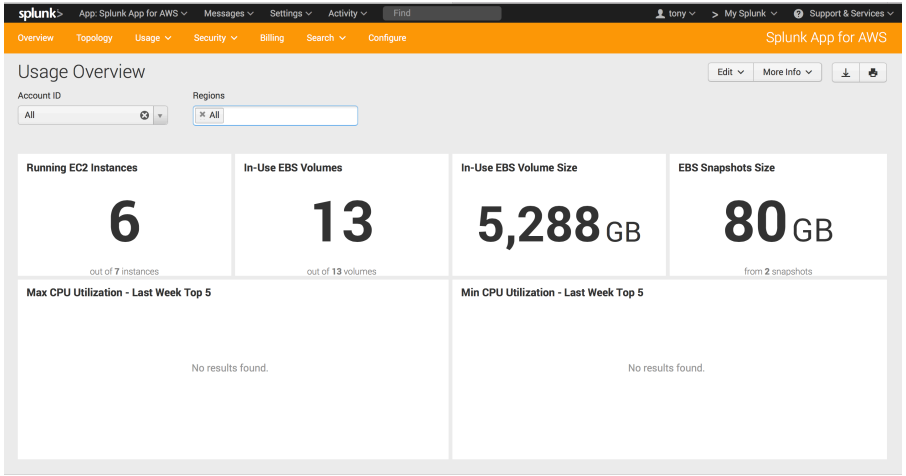
- The overview page shows you on one screen information about Configuration changes, Compute, Network, Storage and Security
- Notable CloudTrail Activity is highlighted on the map
- Drill down on any event and gain detailed information

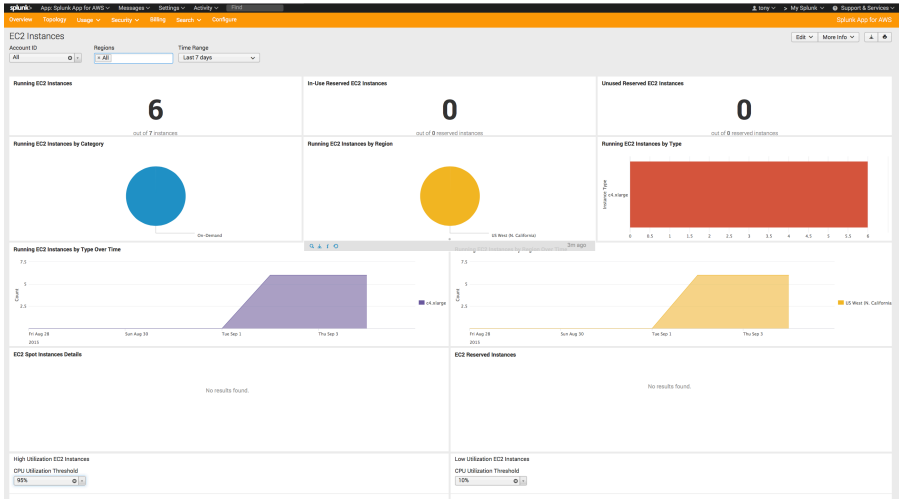
AWS Topology

- Topology view gives you a holistic view of your AWS deployment
- Maps out relationships between all the components, giving you a clear view into the environment
- Customizable views allow you to pick on items and see specific details about those items



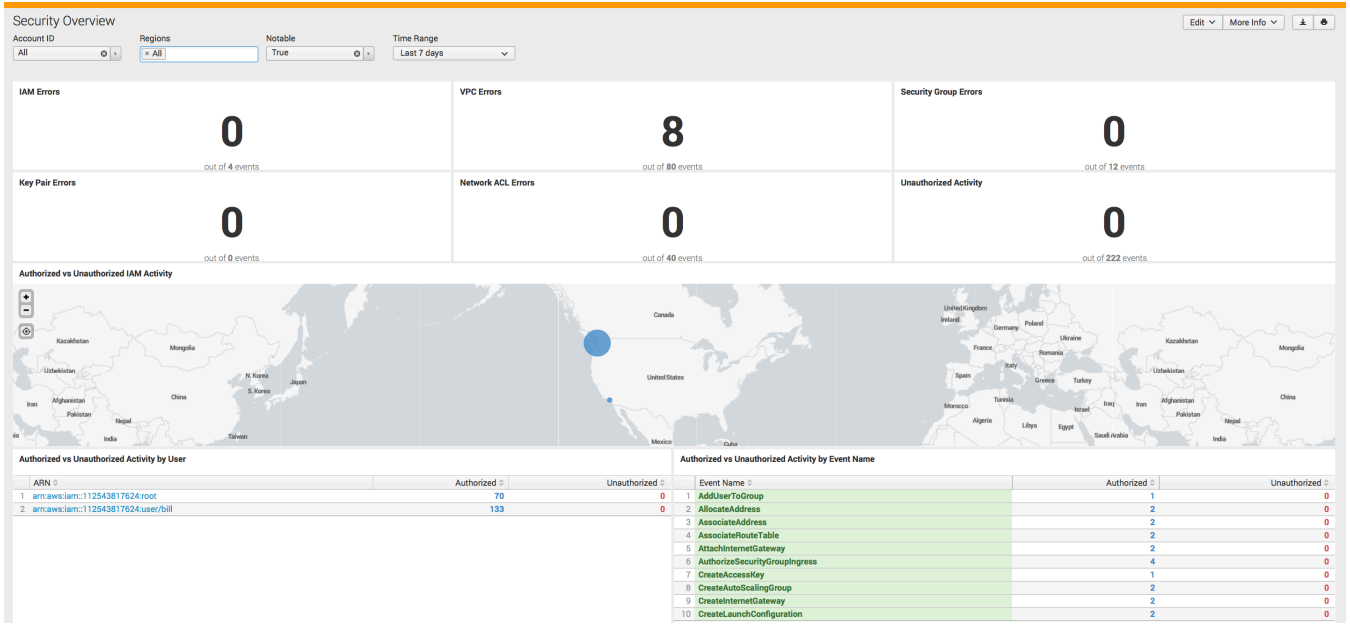
AWS Usage Overview





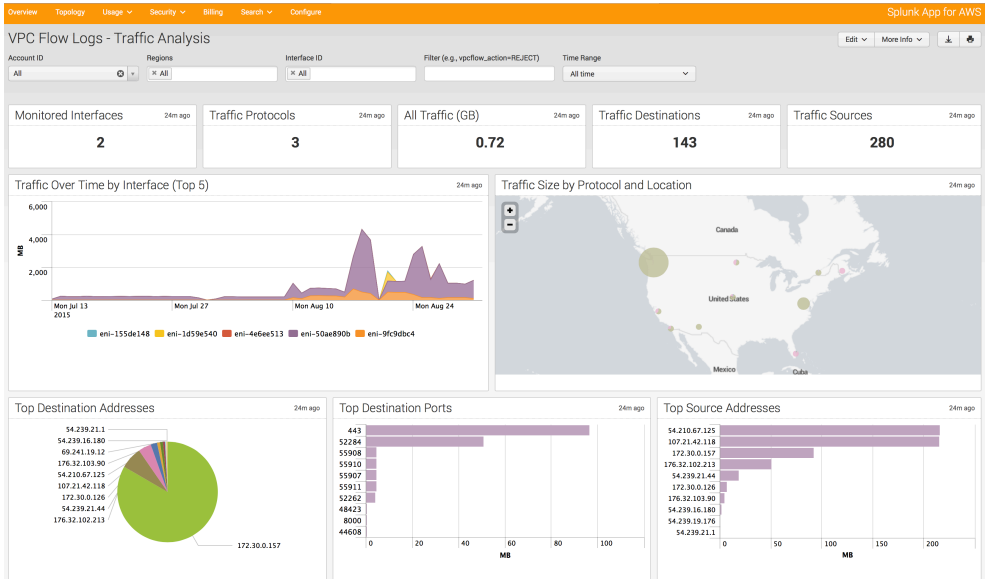
- In one glance, instantly see your EC2 usage
- Click down views jump to interactive dashboards that highlight
- See detailed information about individual EC2 instances
- Drill down into raw search for even more detailed views on your instances
- Detailed EBS Volume data information

AWS Security Overview



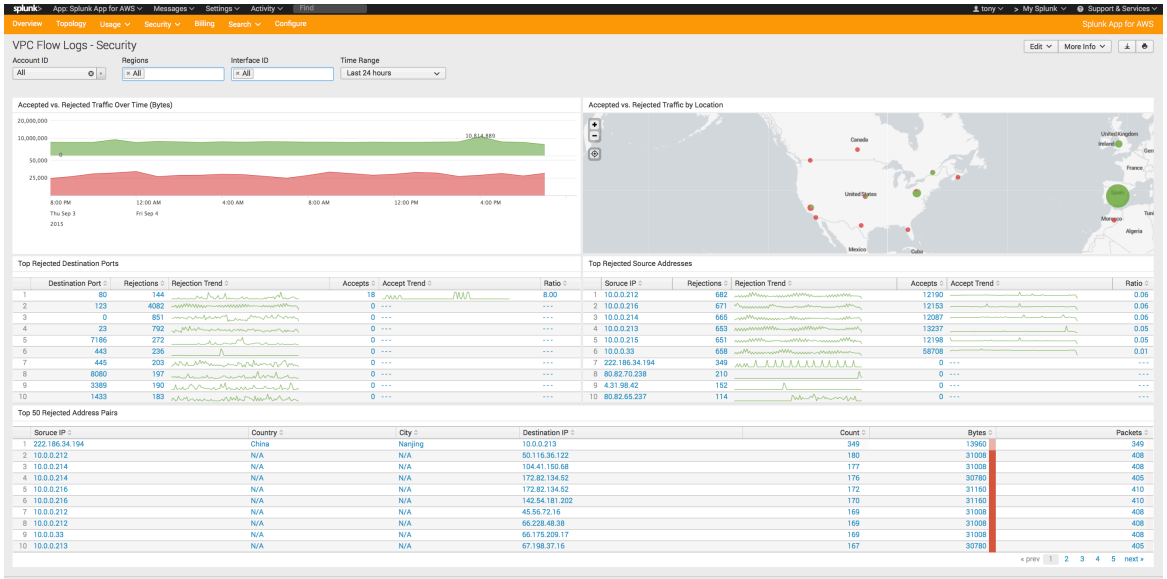
- Quickly see events that impact your AWS security
- Drill down into Authorized vs. Unauthorized Account Activity
- View Errors across VPC, IAM, Key Pairs, Network ACL's and Security Groups
- Map user activity
- Get a list of events happening in your deployment

VPC Flow Data - Traffic



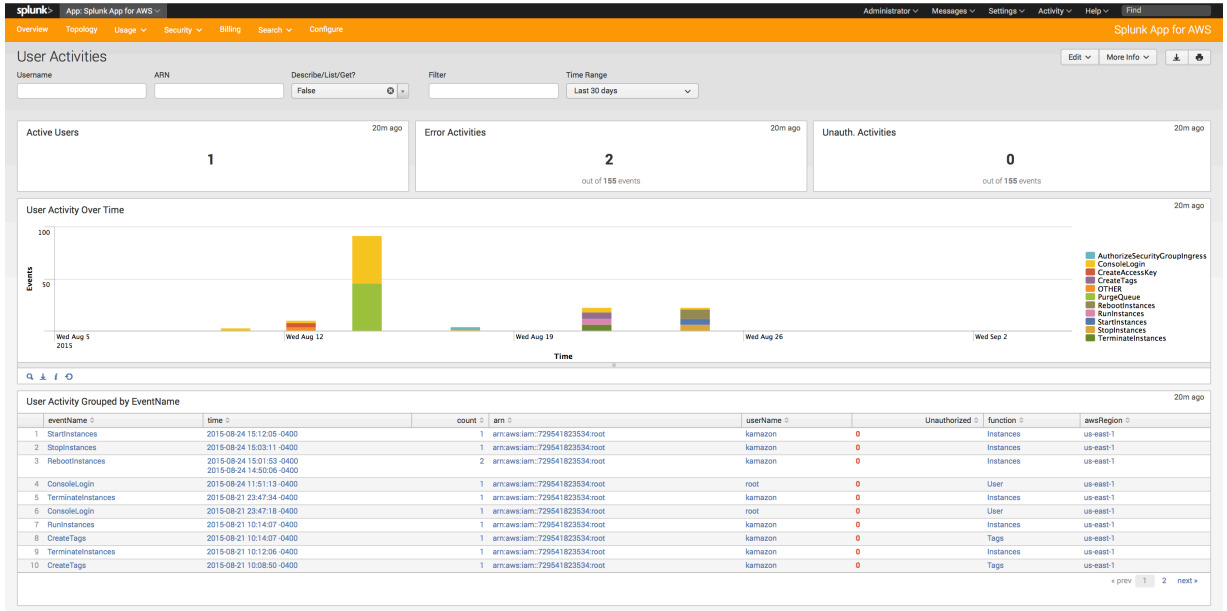
- View VPC Flow Logs for Traffic Analysis
- Drill down into individual network interfaces
- View total traffic flowing in / out of your AWS VPC's
- See top source / destination and IP Addresses and ports

VPC Flow Data - Security



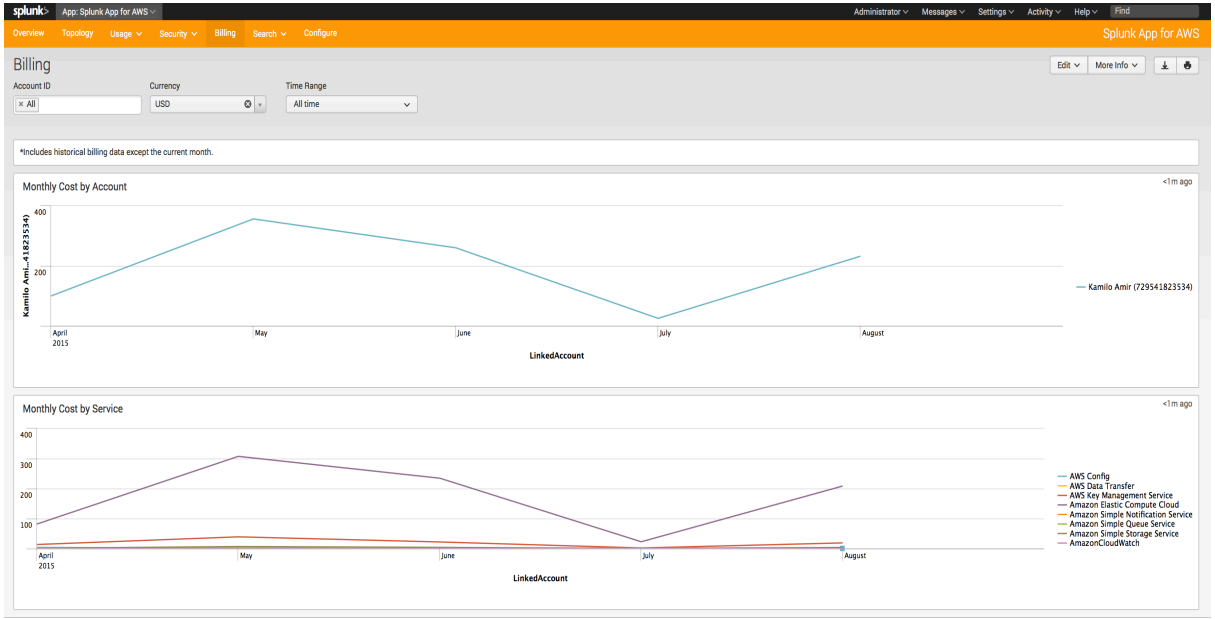
- View VPC Flow Logs for Security Analysis
- Drill down into rejected vs. accepted traffic
- View top Source Country and City information
- See top source / destination and IP Addresses and ports

AWS User Activities



- Quickly see the number of active users logged into the system
- Get alerted on unauthorized user activities
- See what ARN's are being used to access services and the correlated functions
- Create alerts for any user action

AWS Billing and the Splunk App for AWS



- Leverages data being stored in S3 buckets for your AWS bills
- Dashboards show you the current spend on your AWS deployment
- You can see costs by Month, user accounts, services etc.
- Create custom alerts when your bills are climbing higher than expected.

Troubleshooting

splunk>

Troubleshooting

- Check the permissions on the AWS user that you are using to collect logs. Default is no access for users and resources. **Deny takes precedence**
- Splunk the logs **index=_internal sourcetype=aws***
- Dashboards not populating in the AWS app – make sure data is flowing to the index the dashboard search expects it in
- Python scripts log error messages, like Access Denied, SQS not found, etc.

- http://docs.splunk.com/Documentation/AddOns/latest/AWS/Troubleshooting

Building your own Modular Input for AWS

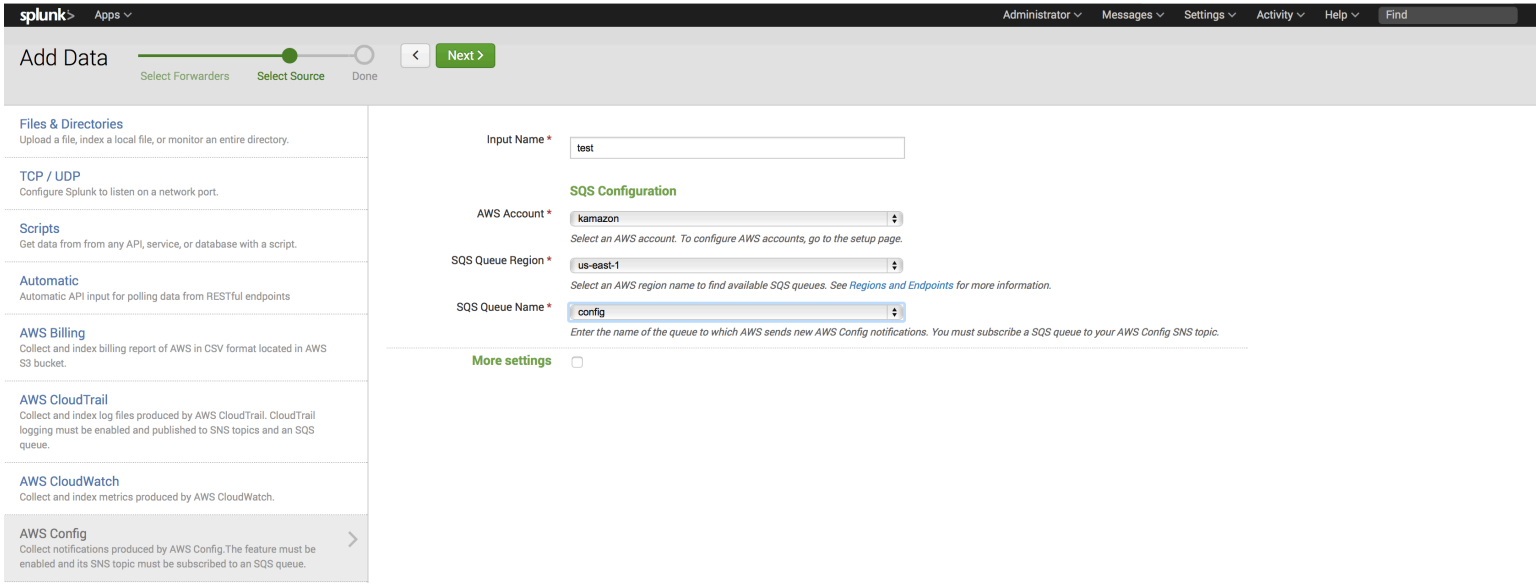
splunk>

Python Script

- Create Python Script that talks to Boto SDK
- Use **aws_s3.py** as a template to collect data from S3 bucket
- Use **aws_config.py** as a template to collect data from SQS
- Modify it with specific output from either JSON, Key Value Pairs, CSV, etc.
- ($SPLUNK_HOME/etc/apps/Splunk_TA_aws/bin/)

Data_inputs_aws-yourapp.xml

- Located in $SPLUNK_HOME/etc/apps/Splunk_TA_yourapp/default/data/ui/manager
- This XML file will populate the Data Inputs Screen:



Props.conf

- Located in $SPLUNK_HOME/etc/apps/Splunk_TA_yourapp/default/
- This config file will tell Splunk how to parse the data from the SQS

JSON Formatted

```
###################################
###       AWS YourApp               ###
###################################

[aws:yourapp]
INDEXED_EXTRACTIONS = JSON
TIME_PREFIX = \"TimeStamp\"\s*\:\s*\"
TIME_FORMAT = %Y-%m-%dT%H:%M:%S%Z
MAX_TIMESTAMP_LOOKAHEAD = 28
```

KVP Formatted

```
###################################
###       AWS YourApp               ###
###################################

[aws:dome9]
SHOULD_LINEMERGE = false
TRUNCATE = 8388608
TIME_PREFIX = \"TimeStamp\"\s*\:\s*\"
TIME_FORMAT = %Y-%m-%dT%H:%M:%S%Z
MAX_TIMESTAMP_LOOKAHEAD = 28
```

Inputs.conf

- This file will be populated once you go through the Data Inputs Wizard

```
[aws_yourapp]
aws_account =
sourcetype = aws:yourapp
#exclude_describe_events = true
enable_additional_notifications = false
queueSize = 128KB
persistentQueueSize = 24MB
interval = 30
```

README/inputs.conf.spec

- Located in $SPLUNK_HOME/etc/apps/Splunk_TA_yourapp/README
- File used to coincide with the inputs that are specified in the XML file ($SPLUNK_HOME/etc/apps/Splunk_TA_yourapp/default/data/ui/manager/data_input_yourapp.xml)

aws_yourapp://<name>]
aws_account = AWS account used to connect to AWS
aws_region = AWS region of log notification SQS queue
sqs_queue = Starling Notification SQS queue
enable_additional_notifications = Enable collection of additional helper notifications

Imitation is the best form of flattery

- Just copy the Splunk_TA_aws directory with all the python scripts for the Boto SDK ☺
- Add your custom scripts, config files and XML files

Thanks!

splunk>