Make It Rain

How to save money monitoring, managing and securing your cloud using the Splunk App for AWS

Joshua McQueen | CTO, Arcus Data

September 2018 | Version 1.0

Forward-Looking Statements

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 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.

splunk> .conf18

JOSHUA MCQUEEN

Arcus Data CTO, Co-Founder

splunk> .conf18

Speaker Bio

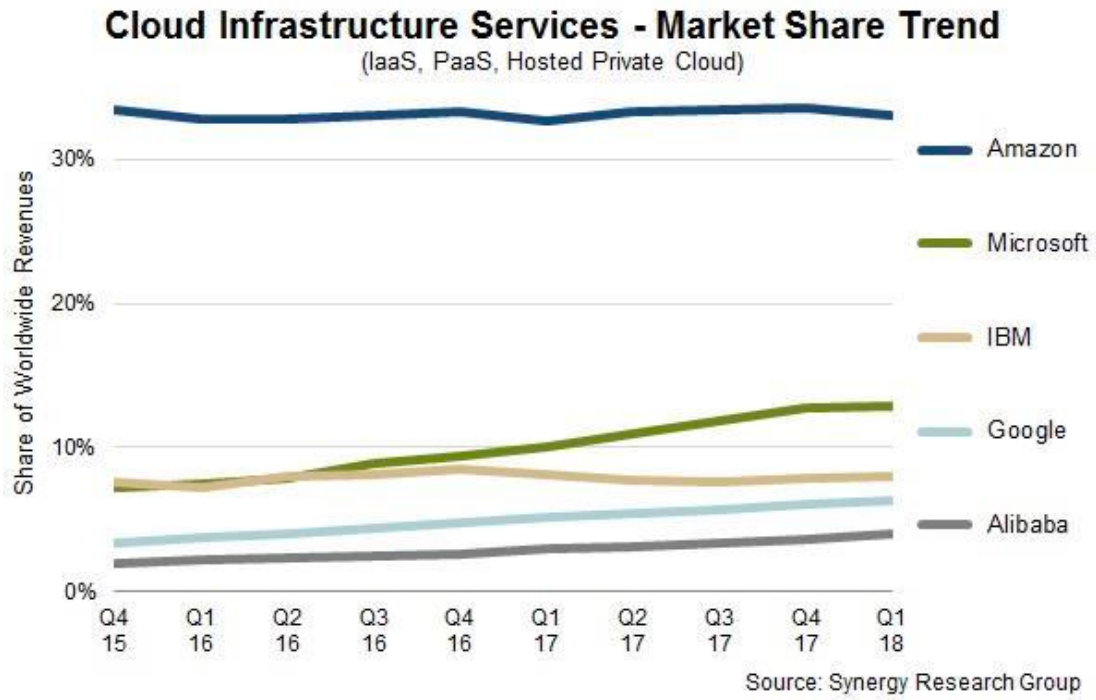
- Joshua McQueen
- CTO and Co-founder of Arcus Data
- Splunk Professional services consultant for 8 years
- Implemented Splunk for over 200 customers across all industries
- Expert in: Splunk, Automation, Cloud Security

“Cloud computing market projected to reach $411B By 2020.”

- Gartner Publication

AWS Meteoric Rise

- Amazon Web Services experiences blistering growth with jaw dropping statistics:
  - US Government now has Secret, Classified, and Sensitive regions
  - AWS has 5 times more deployed cloud infrastructure as their next 14 competitors ...combined
  - Highly regulated industries: Financial Services, Energy, Healthcare
  - AWS supports over 600 government agencies and 2400 .edu

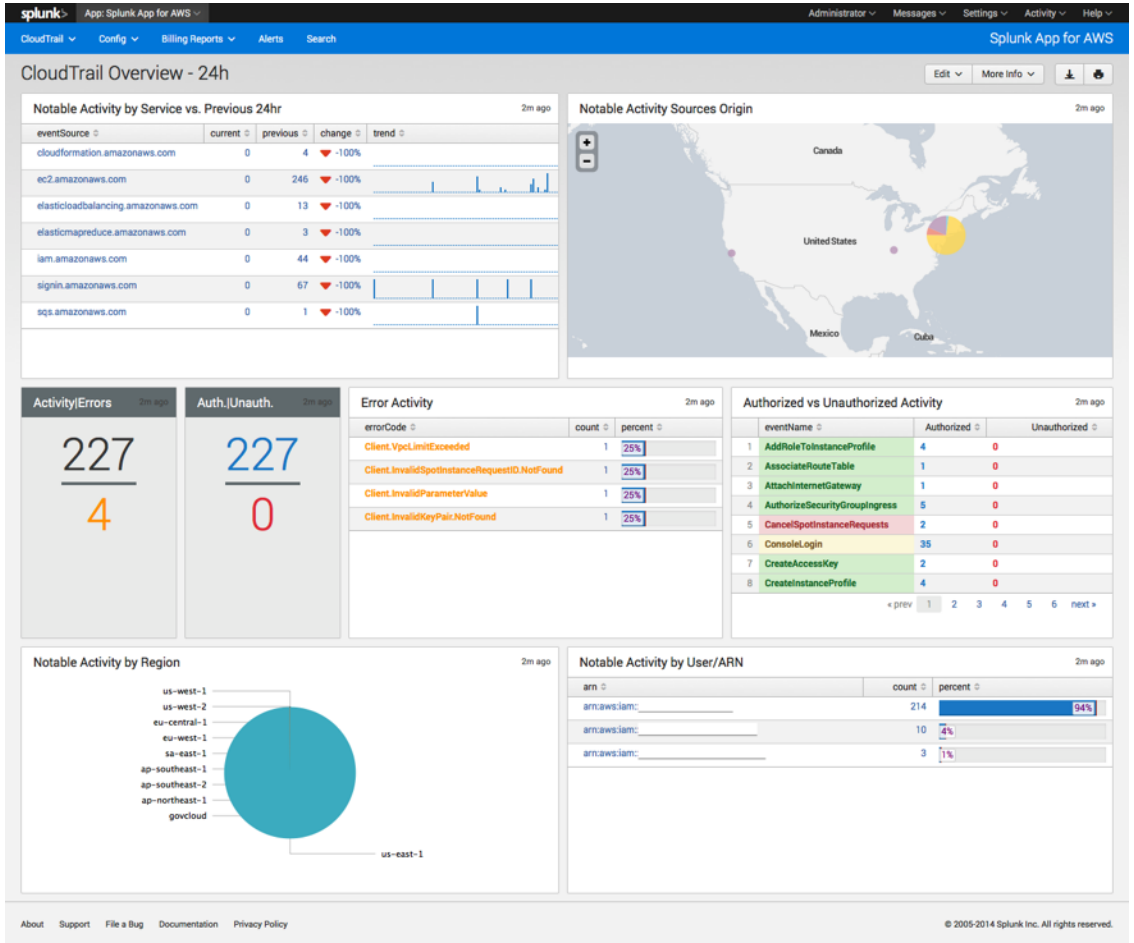


Monitoring and Securing Cloud is CRITICAL.

splunk> .conf18

Why We Need to Monitor?

- 5-10 Years ago there were security concerns with “shared infrastructure”
- Now, securing and monitoring cloud is part of everyday business
- Companies are migrating mission critical applications and workloads
- Analyze security risk, resource usage, performance
- Make decisions across multiple accounts in different regions
- Billing and Cost Control



Agenda for Today

This presentation will focus on three areas:

1. **CloudTrail**
2. **VPC Flow (new!)**
3. **CloudWatch**

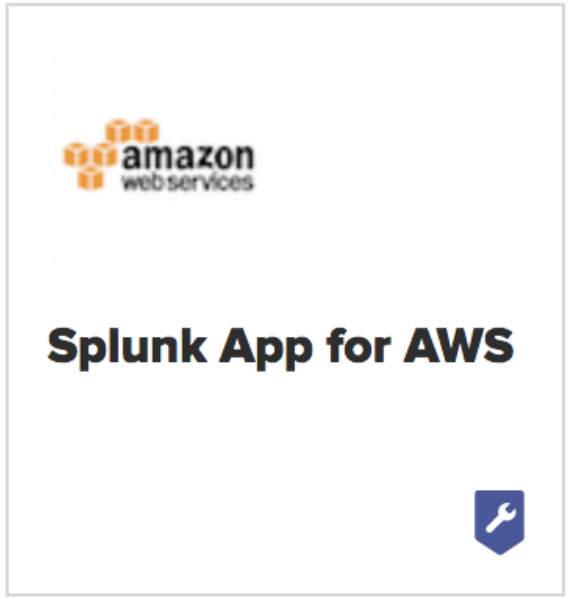
- **Finally, we'll wrap up with real-world customer use cases.**

Data source	Source type	Description
Config	`aws:config`	Configuration snapshots and historical configuration data from the AWS Config service.
	`aws:config:notification`	Configuration change notifications from the AWS Config service.
Description	`aws:description`	Descriptions of your AWS EC2 instances, reserved instances, and EBS snapshots, used to improve dashboard readability.
Config Rules	`aws:config:rule`	Compliance details, compliance summary, and evaluation status of your AWS Config Rules.
Inspector	`aws:inspector`	Assessment Runs and Findings data from the Amazon Inspector service.
CloudTrail	`aws:cloudtrail`	AWS API call history from the AWS CloudTrail service.
CloudWatch Logs	`aws:cloudwatchlogs`	Data from the CloudWatch Logs service.
	`aws:cloudwatchlogs:vpcflow`	VPC flow logs from the CloudWatch Logs service.
CloudWatch	`aws:cloudwatch`	Performance and billing metrics from the AWS CloudWatch service.
Billing	`aws:billing`	Billing reports that you have configured in AWS.
	`aws:billing:cur`	Cost and Usage Reports that you have configured in AWS
S3	`aws:s3`	Generic log data from your S3 buckets.
	`aws:s3:accesslogs`	S3 access logs.
	`aws:cloudfront:accesslogs`	CloudFront access logs.
	`aws:elb:accesslogs`	ELB access logs.
	`aws:cloudtrail`	Cloudtrail data
Kinesis	`aws:kinesis`	Data from Kinesis streams.
SQS	`aws:sqs`	Generic data from SQS.

splunk> .conf18

Splunkbase Apps

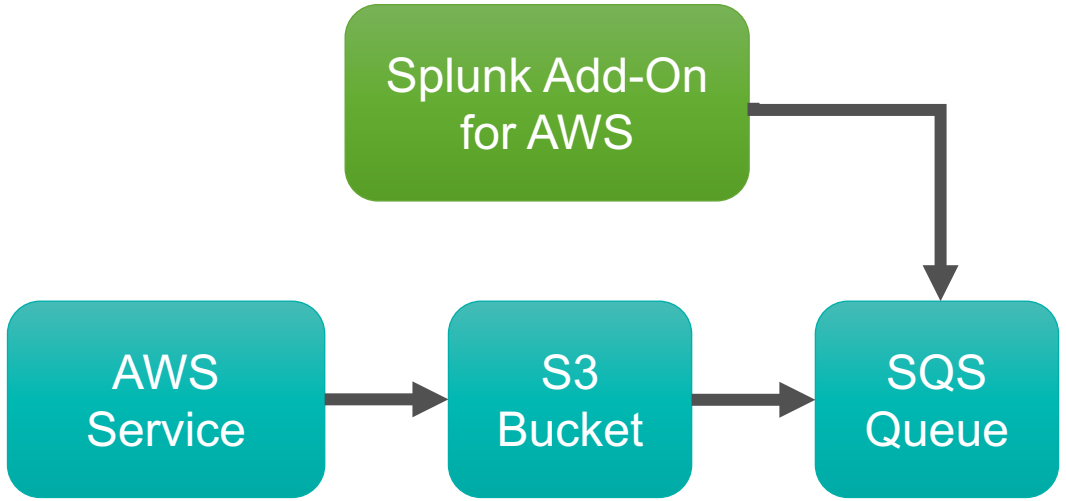
Splunk **Add-on** for
Amazon Web Services
Version 4.5.0

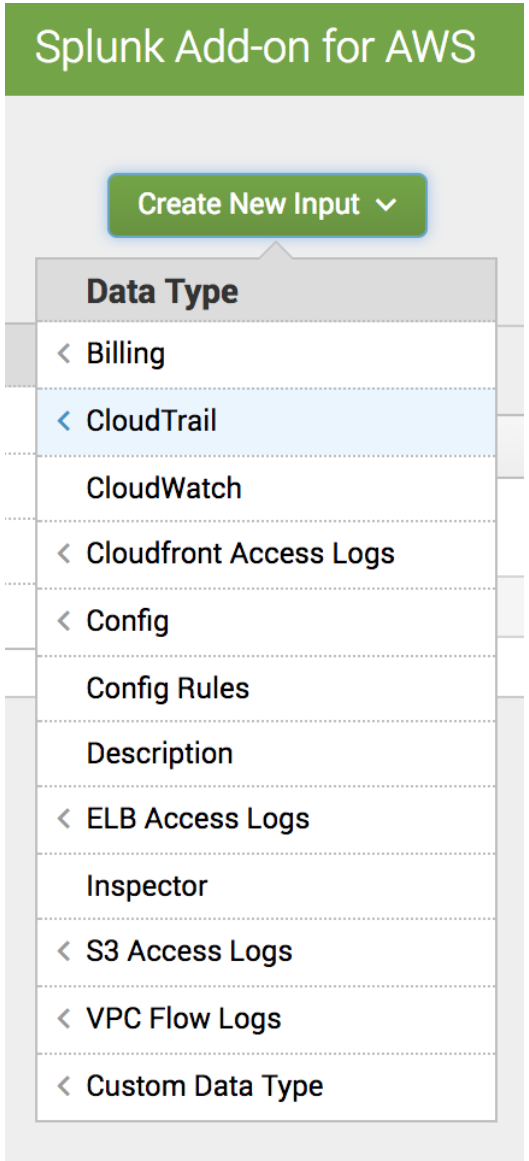


Splunk **App** for
Amazon Web Services
Version 5.1.1

AWS Inputs

- Getting AWS logs into Splunk can be *confusing*
- There are different methods for each sourcetype
- **Best Practice is to use SQS-Based S3**
- **High scale, stateless, near real-time processing:**





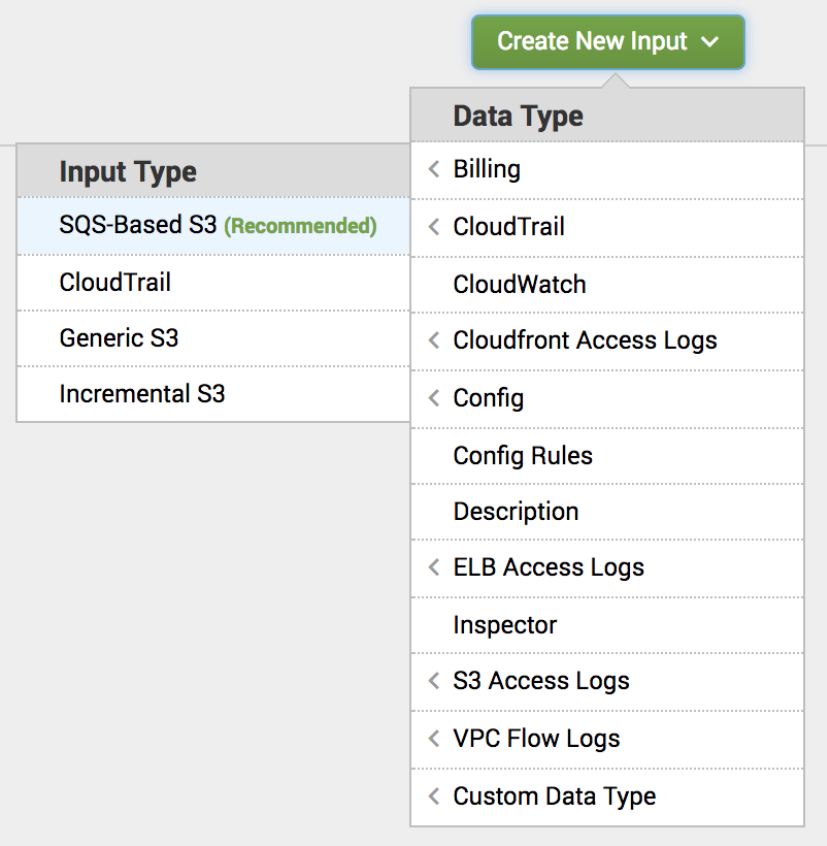
CloudTrail – AWS Setup

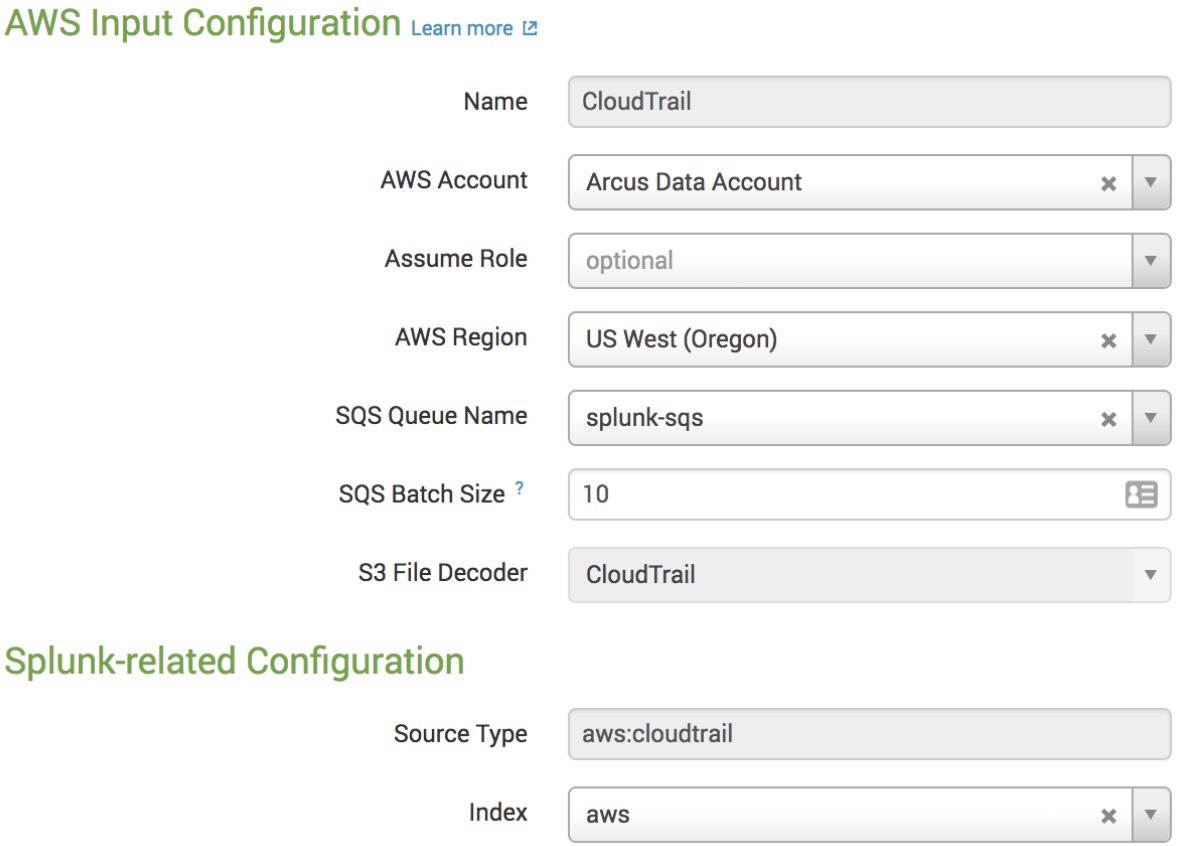
Let's work backwards:

1. Create Dead-letter queue THEN regular SQS queue
   - Regular queue needs visibility timeout of 5+ mins
   - Under redrive policy, set max receives to 1
2. Create new CloudTrail (or enable existing one)
   - Write to S3 bucket
3. Update SQS queue to allow S3 bucket notifications
4. Update S3 events to send notifications to SQS – ObjectCreate(all)

CloudTrail – Splunk Setup

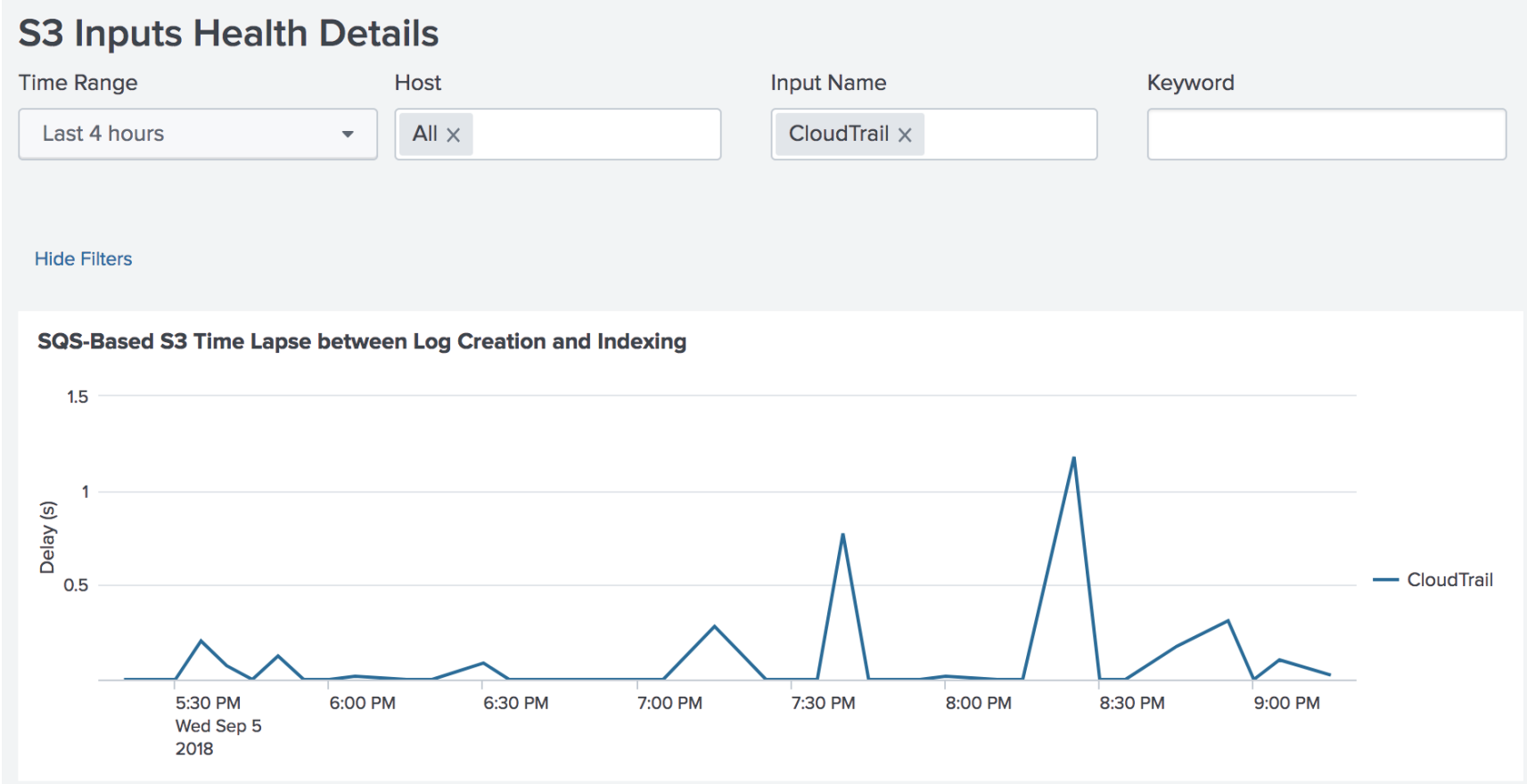
- Create New Input > CloudTrail > SQS-Based S3





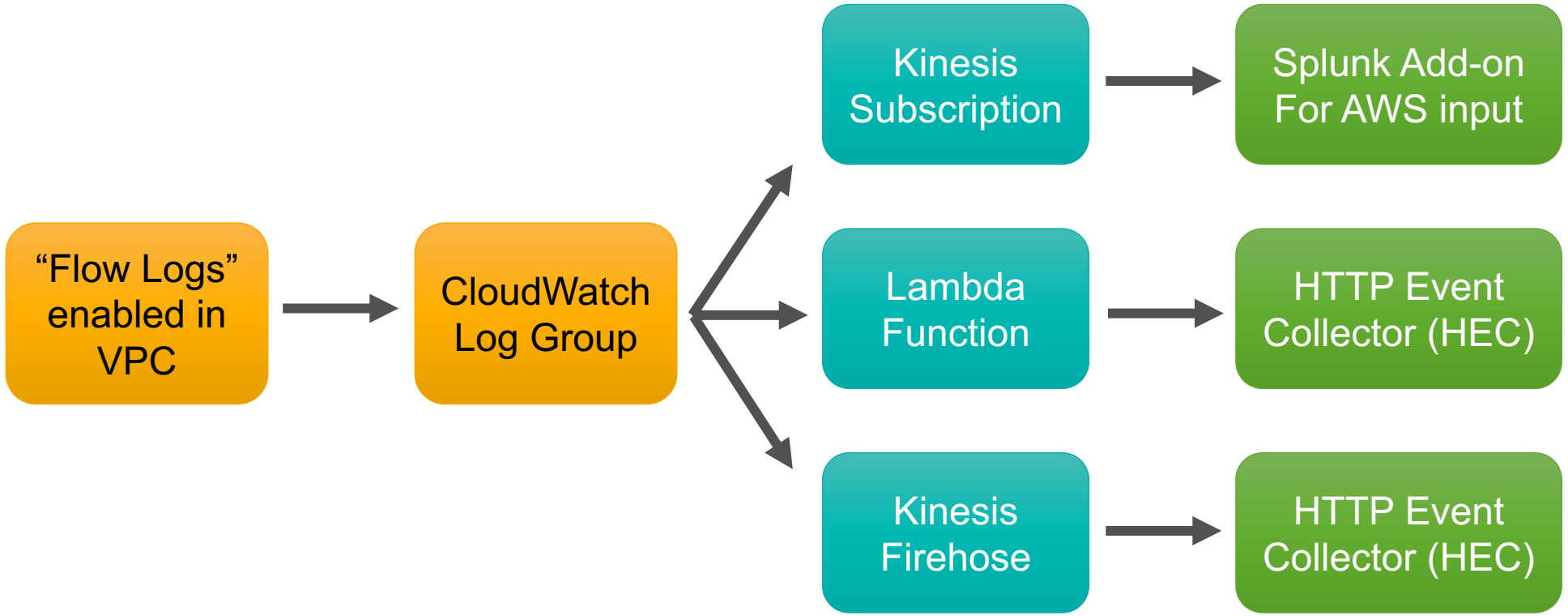
CloudTrail - Testing

- Splunk Add-on for AWS > Health Check > S3 Inputs



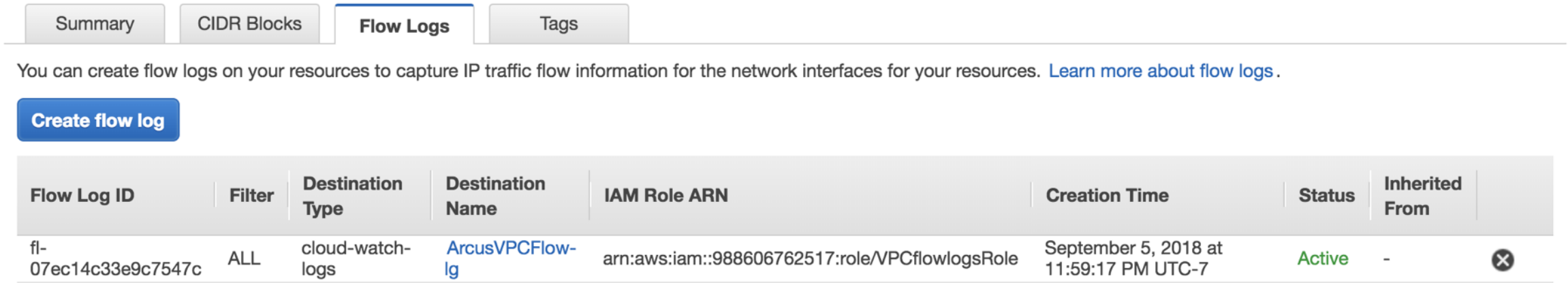
VPC Flow - Architecture

- There are **three** ways to get VPC Flow logs into Splunk:



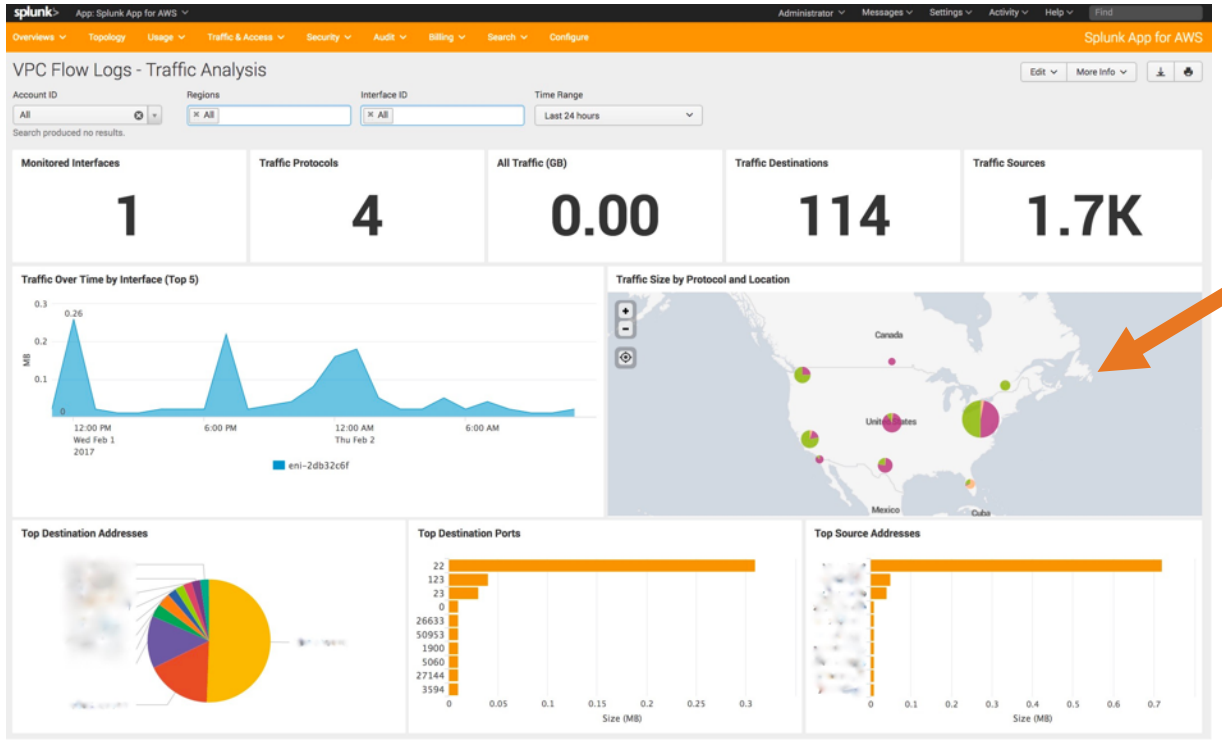
VPC Flow – AWS Config

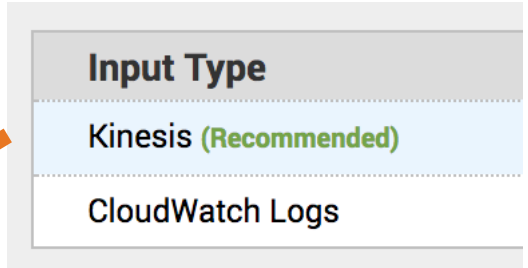
- "Create Flow Log" on VPC you want to monitor
- Setup the appropriate access permission and roles
- Create the Kinesis data stream
- Create the Log Group
- Follow AWS command line instructions here



VPC Flow – Splunk Config

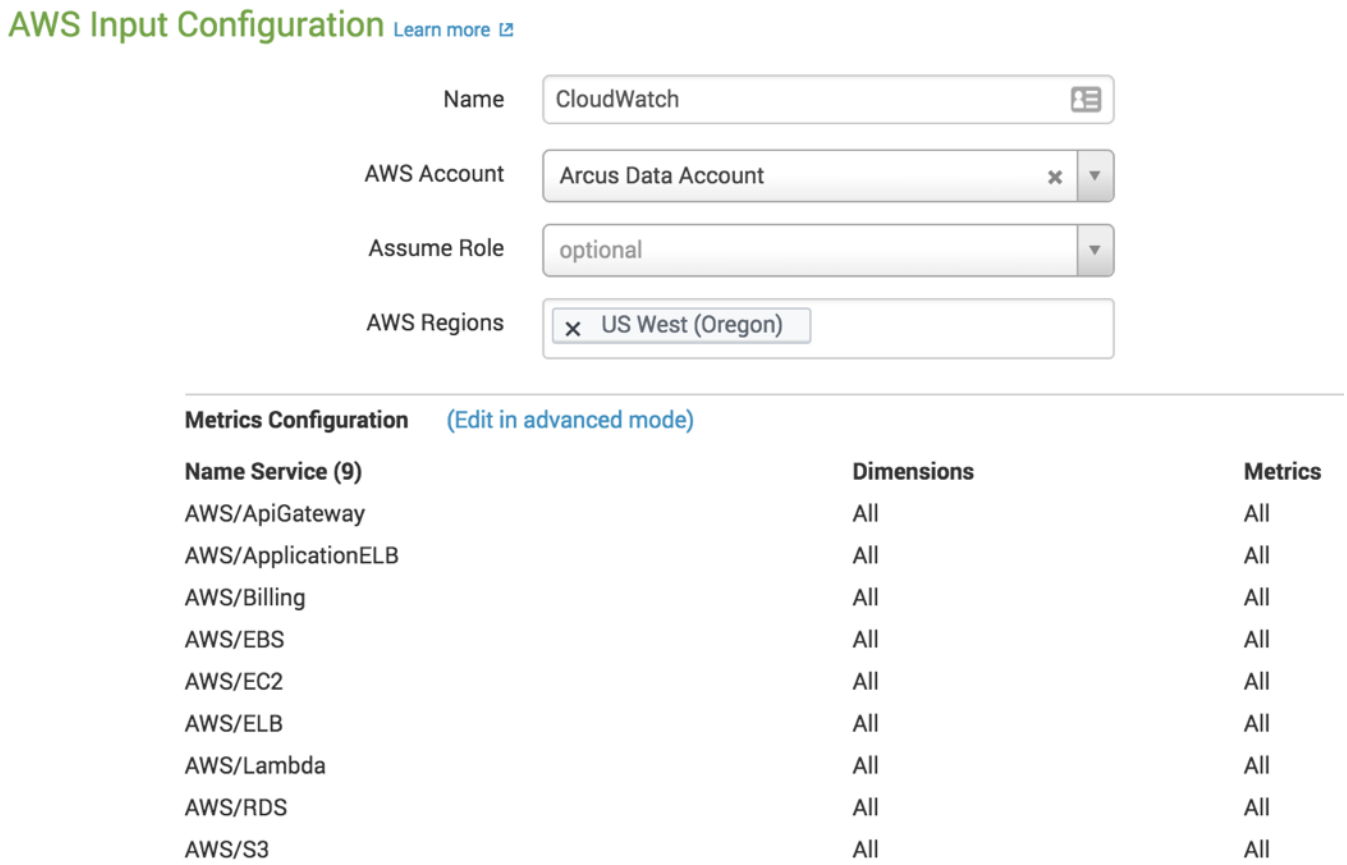
- Splunk App for AWS > Create Input > VPC Flow > Kinesis
- Test using Traffic Analysis dashboard:

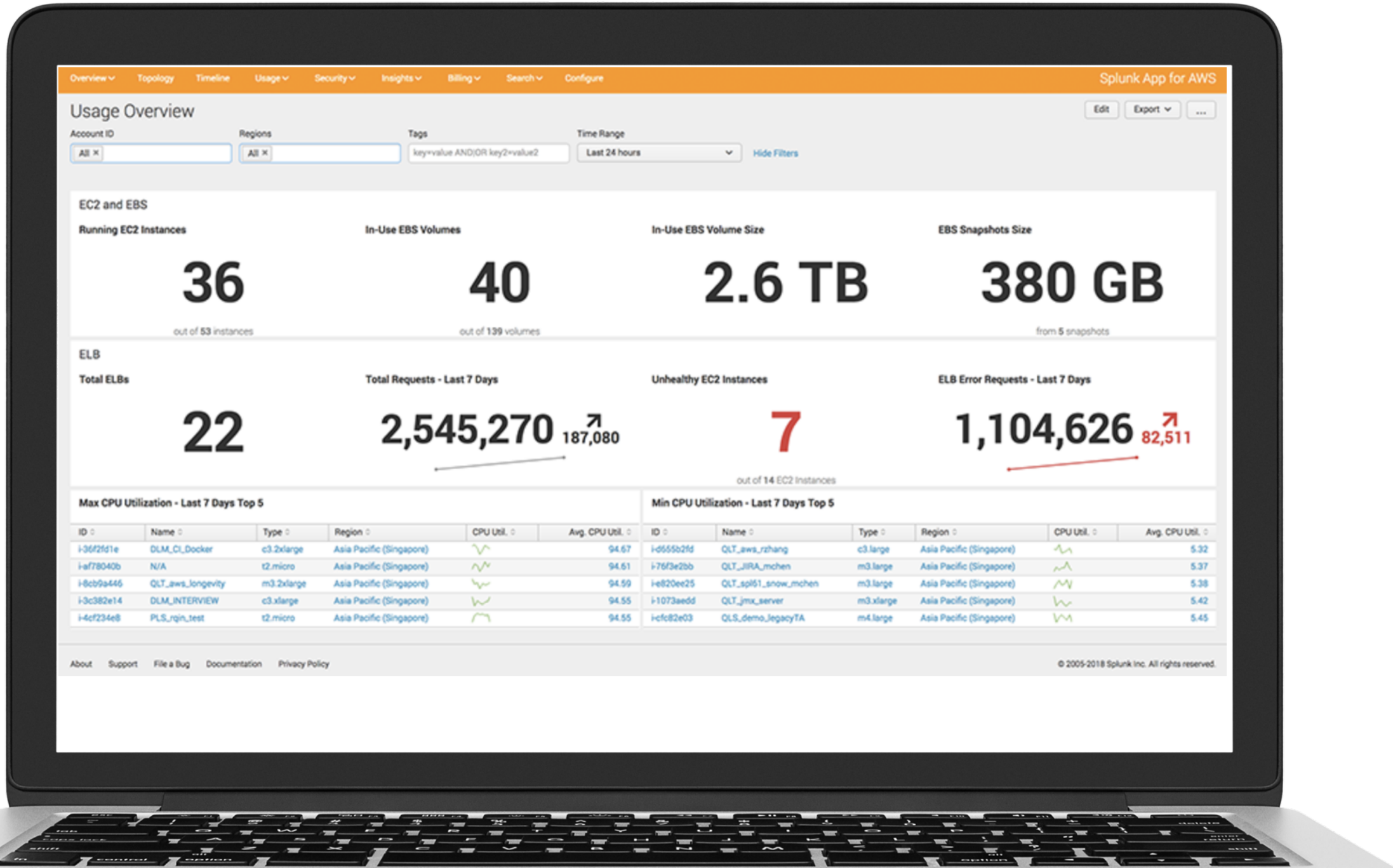




AWS CloudWatch

- Saved the easiest for last! Enable using “Create Input”





Use Cases

Retailer Enables Realtime VPC Monitoring

- Consumer retailer with 150+ stores
- Lines of business through mobile apps and .COM website
- Customer had issues monitoring when cloud credit card processor is down
- Potential Security Threat? Network Issue?
- $$$ Expensive – Root cause analysis took days to complete, security team, network team, incident management was involved

Solutions:

- Using VPC Flow to track (in real-time) the network links and application health
- Isolate the root cause quickly using saved searches and dashboads

splunk> .conf18

Cost Savings – Gaming Company

- Highly anticipated game launch, blockbuster title
- All the back-end servers run in AWS across all regions
- Elastic Load Balancing (ELB) ran out of “reserved instances”

Solutions:

- Use predictive forecasting
- Setup alerts in budget planner
- Reserved Pricing vs. On Demand

Monitor Arcus Insights Platform

- At Arcus Data, we have our own Saas Cloud Platform
- Security and protection of client data is highest priority!
- Engineers rely heavily on Automation: CloudFormation, Terraform, Ansible
- DevOps Workflow: Deploy, Configure, Test, Terminate

Solutions:

- Use Splunk to analyze network traffic, monitor CPU usage, IAM credentials
- Quickly identify bitcoin mining & other security threats
- Monitor assets looking for “publicly shared” permissions
- Developed team dashboards to track individual engineer’s cloud spend

Key Takeaways

Get the most from AWS

1. Holistic AWS monitoring across all accounts, resources, and regions
2. Enable logging through S3 & SQS
3. Enhance security with VPC Flow
4. Save money through billing and cost management

We're Here to Help

ARCUSDATA

Product Resale

Professional Services

Managed Services

aws

Google Cloud Platform

Microsoft Azure

splunk>

ANSIBLE

CHEF

puppet labs

splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app

Resources

- Links:
  - Add-on: https://splunkbase.splunk.com/app/1876/
  - AWS App: https://splunkbase.splunk.com/app/1274/

- VPC Flow Video: https://www.youtube.com/watch?v=U_esFvx6GHY