

Splunk & AWS

Gain real-time insights from your data at scale

Ray Zhu | Product Manager, AWS

Elias Haddad | Product Manager, Splunk

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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Agenda

- ▶ Current Splunk ingestion landscape for AWS
- ▶ Current challenges
- ▶ New Solution
- ▶ Demo
- ▶ Q&A

130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=Q1P756j555510N10=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=51-98&product_id=51-98"
130.60.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=Q1P756j555510N10=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=51-98"
130.60.4 - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=51-98&product_id=51-98"
130.60.4 - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 408 125.17 "http://buttercup-shopping.com/new?category_id=5198"
130.60.4 - [07/Jan 18:10:57:156] "GET /cart.do?action=refresh&itemId=51-98 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/new?category_id=5198"
130.60.4 - [07/Jan 18:10:57:156] "GET /category.screen?category_id=5198 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/new?category_id=5198"

Monitored by **splunk**>

Splunk Cloud Available Worldwide



Splunk Portfolio of AWS Solutions

End-to-End AWS Visibility



App for AWS

Available on Splunk Enterprise, Splunk Cloud and Splunk Light

AWS

Integrations

AWS Lambda, IoT, Kinesis, EMR, EC2 Container Service

Self-deployed AMIs or SaaS on AWS Marketplace



AMI on AWS Marketplace



SaaS Contract Billed through Marketplace



Insights for AWS Cloud Monitoring

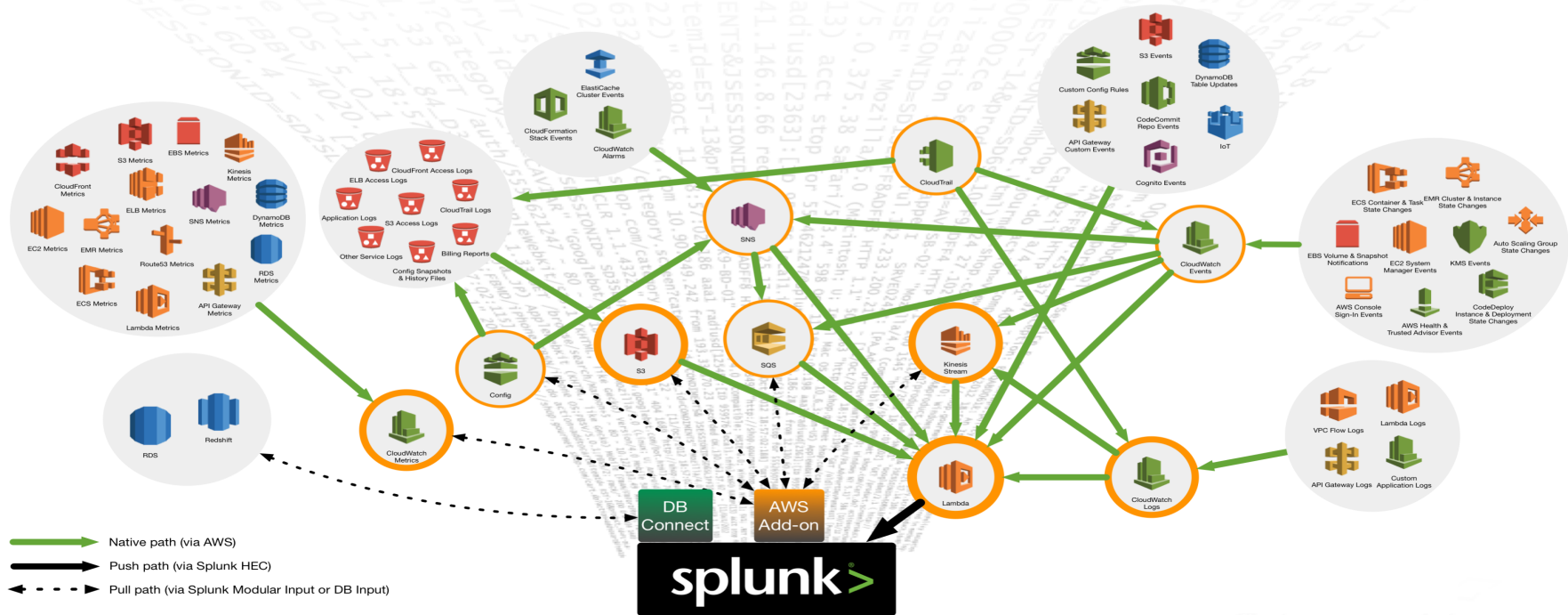
AMI on AWS Marketplace

AWS-based SaaS



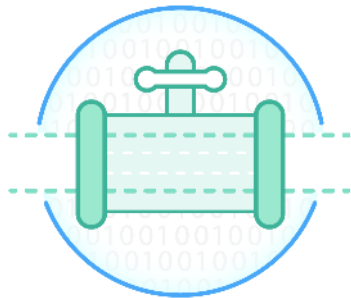
Benefits of Splunk Enterprise as SaaS

Current Splunk GDI Landscape for AWS



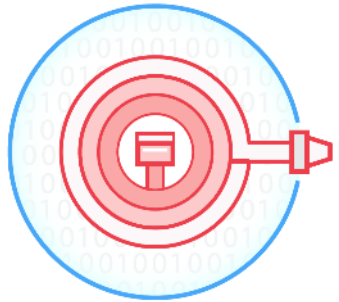
Need for New Solution

Amazon Kinesis



Kinesis Streams

Stores data as a continuous replayable stream for custom applications



Kinesis Firehose

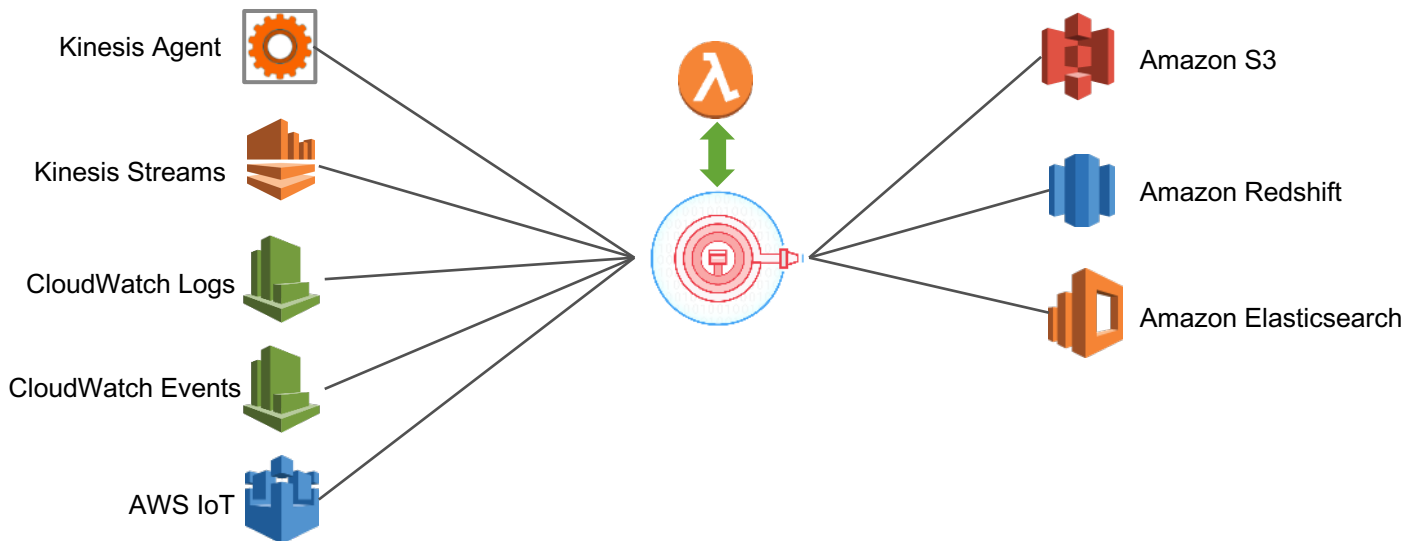
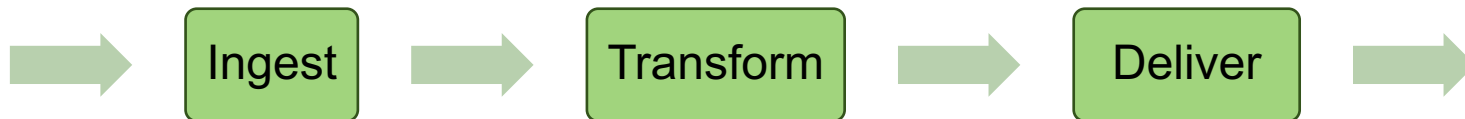
Load streaming data into Amazon S3, Amazon Redshift, and Amazon Elasticsearch Service



Kinesis Analytics

Analyze data streams using standard SQL queries

Current State of Kinesis Firehose

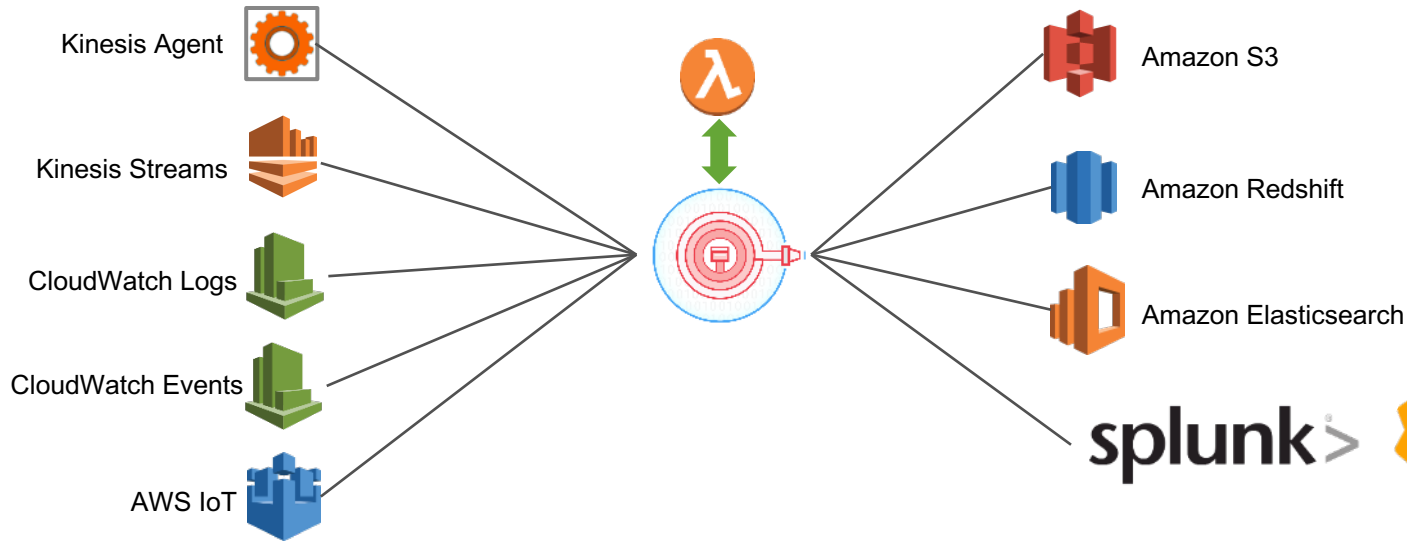
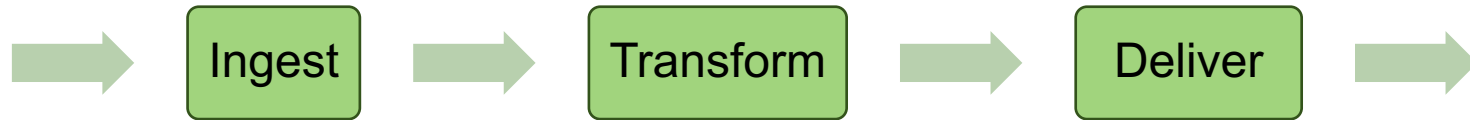


130.60.4 - [07/Jan 18:10:57:153] "GET /category/screen?category_id=Q1F7s&j55510N10=5D55L9FF1ADFF3 HTTP/1.1" 404 720 "http://butte...
138.241.230.82 - [07/Jan 18:10:57:153] "GET /product/screen?product_id=F5L8H-B18&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 404 3322 "http://butte...
1317.27.160.0 - [07/Jan 18:10:57:153] "GET /product/screen?product_id=F5L8H-B18&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://butte...
vitenid=EST-10&product_id=RP-L1-02" 468 125.17 "c.789) "GET /cart.do?action=view&itemid=EST-10&product_id=RP-L1-02" 200 1318 "http://butte...
shopping.com/purchase&...
shopping.com/purchase&...

Our Answers to Challenges

- ▶ Reliability, scalability and fault tolerance challenges
 - Extremely reliable with underlying infrastructure operating in three different AZs
 - Extremely durable with three copies of same data in three different AZs
 - Temporarily holds and buffers data to absorb back pressure
 - Data backup to Amazon S3 upon failure
- ▶ Management overhead of data collection nodes in existing solution
 - Serverless with no resource provision or management overhead
- ▶ Delayed event delivery due to poll based ingestion
 - Push delivery with configurable buffer size and interval
- ▶ API throttling with poll based data ingestion
 - Horizontally scalable with no limit

Kinesis Firehose With Splunk Delivery



```

128.60.4 - [07/Jan 18:10:57:153] "GET /category/screen?category_id=01f75b3555101d5d551a7f18a0ff18 HTTP/1.1" 404 720 "http://butte
128.241.230.82 - [07/Jan 18:10:57:153] "GET /product/screen?product_id=f5d818f3555101d5d551a7f18a0ff18 HTTP/1.1" 404 3322 "http://butte
1317.27.160.0 - [07/Jan 18:10:57:153] "GET /product/screen?product_id=f5d818f3555101d5d551a7f18a0ff18 HTTP/1.1" 200 1318 "http://butte
vitenId=EST-10&product_id=RP-L1-02" 468 125.17 "c:8789) "GET /cart.do?action=view&itemId=EST-10&product_id=RP-L1-02"
action=shopping_id=RP-L1-02" 468 125.17 "c:8789) "GET /category/screen?category_id=5d551a7f18a0ff18 HTTP/1.1" 200 1318 "http://butte
shopping.com/purchase&
  
```

Kinesis Firehose Advantages

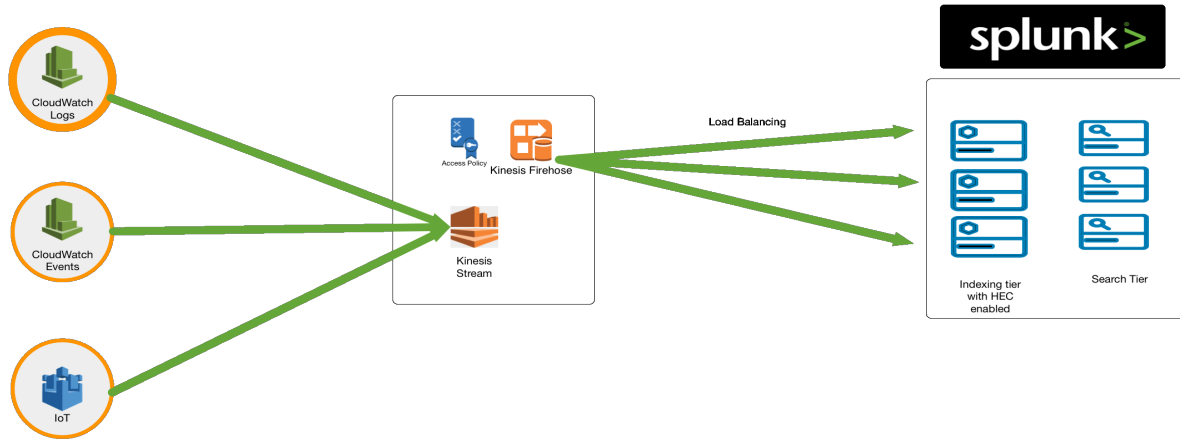
Why should I use Kinesis Firehose versus other ingestion mechanisms for Splunk?

Why Kinesis Firehose

- ▶ Fully managed service with serverless architecture
- ▶ Bypass the need for setting up and managing heavy weight forwarder
- ▶ Extremely scalable and reliable
- ▶ Well integrated with various data sources
- ▶ Easy to use with no programming requirement
- ▶ Ability to transform raw data prior to sending it to Splunk
- ▶ Super low cost - \$0.029 per GB of data ingested

```
130.60.4 - [07/Jan 18:10:57:153] "GET /category/screen?category_id=01f75b355510105D55L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=521-00product_id=521-buttercup-  
130.241.230.02 - [07/Jan 18:10:57:153] "GET /product/screen?product_id=FL-D5H-018JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=521-00product_id=521-buttercup-  
ome NT 5.1: 160.0.0 - [07/Jan 18:10:57:153] "GET /product/screen?product_id=FL-D5H-018JSESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=521-00product_id=521-buttercup-  
//buttercup-shopping.com/r/LI-02" "GET /category/screen?category_id=01f75b355510105D55L9FF1ADFF3 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=521-00product_id=521-buttercup-  
action=purchase.com/r/LI-02" 468 125.17 /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=521-00product_id=521-buttercup-  
shopping_id=RP-LI-02" 468 125.17 /category/screen?category_id=01f75b355510105D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=521-00product_id=521-buttercup-  
buttercup-shopping.com/r/LI-02" 468 125.17 /category/screen?category_id=01f75b355510105D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=521-00product_id=521-buttercup-
```

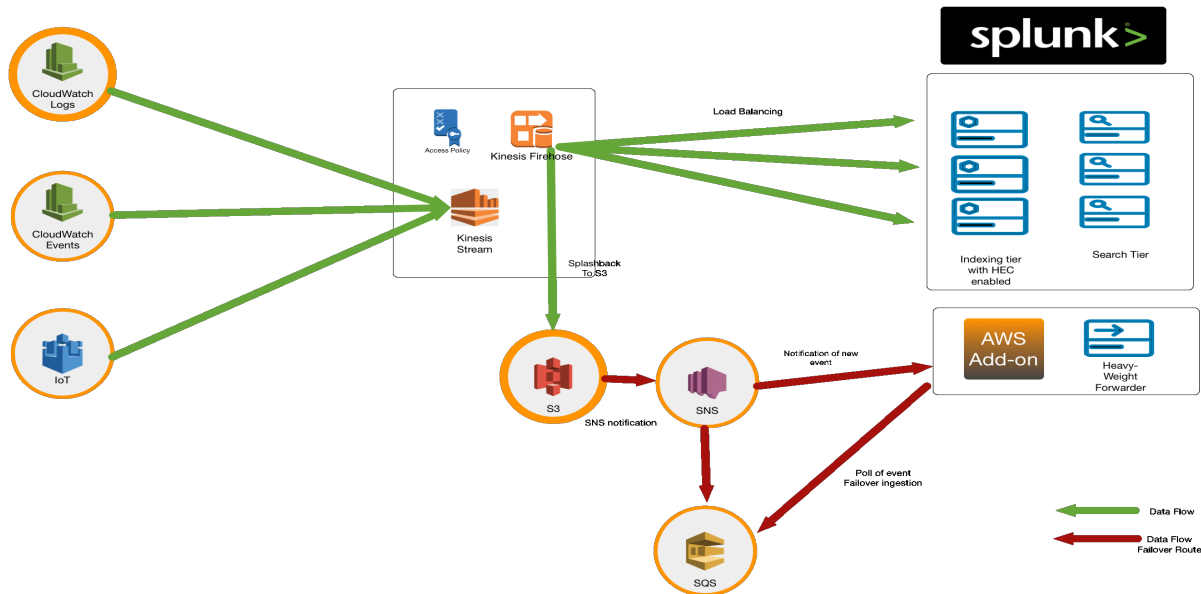
Serverless and Scalable



- ▶ Supports native balancing to indexing tier
- ▶ Supports Splunk Cloud and Splunk Enterprise

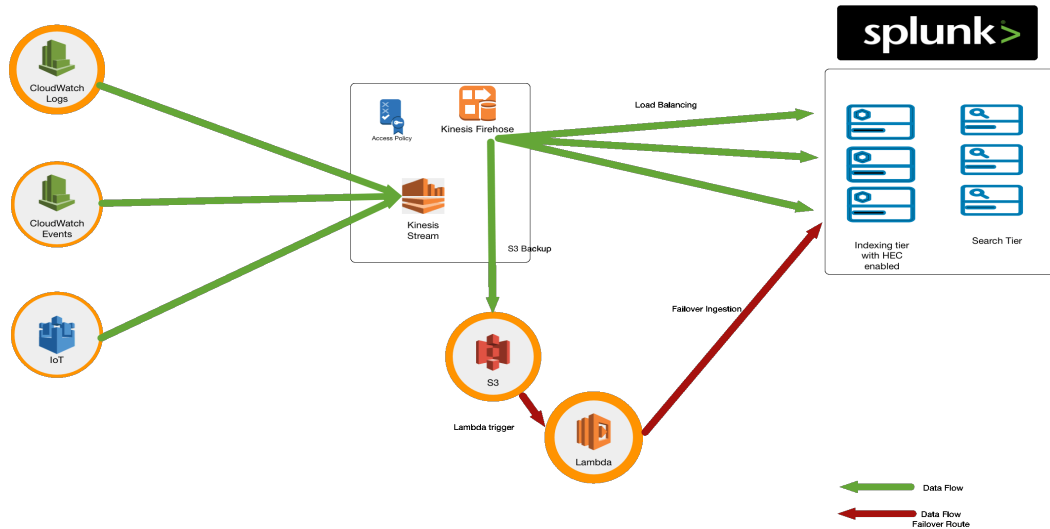
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=01f75b355510105d551a7f18a0ff18 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=51-66product_id=51-66"
138.241.230.82 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-D5H-B18JSESSIONID=5D55L7FF6ADF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=51-66product_id=51-66"
137.27.160.0 - - [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-D5H-B18JSESSIONID=5D55L7FF6ADF9 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=51-66product_id=51-66"
192.168.1.1:51:SVI: NET CLR 1.1.4322] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=51-66product_id=51-66"
103.actioncup-shopping_id=RP-LI-02" 468 125.17 "GET /category.screen?category_id=5166product_id=5166"
103.actioncup-shopping.com/rp-li-02" 468 125.17 "GET /category.screen?category_id=5166product_id=5166"
103.actioncup-shopping.com/rp-li-02" 468 125.17 "GET /category.screen?category_id=5166product_id=5166"
```


Reliable AWS Add-on as Failover



- ▶ Supports delivery acknowledgment. Un-acknowledged events can be persisted to S3 and re-ingested via alternative delivery mechanism.
- ▶ Un-delivered and un-acknowledged events can be ingested from S3 bucket using poll based mechanism (Splunk add-on for AWS)

Reliable Lambda to HEC as Failover



- ▶ Un-delivered and un-acknowledged events can be ingested from S3 using lambda for full push-based architecture.
- ▶ Lambda can be configured to push data to a failover HEC endpoint

```

120.60.4 - - [07/Jan 18:10:57:153] "GET /category/screen?category_id=01f75b355510N10=5D5L7FF6ADF9 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=53-88product_id=53-88"
128.241.230.82 - - [07/Jan 18:10:57:153] "GET /product/screen?product_id=FL-D5H-D18JSESSIONID=5D5L7FF6ADF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=53-88product_id=53-88"
1317.27.160.0 - - [07/Jan 18:10:57:153] "GET /product/screen?product_id=FL-D5H-D18JSESSIONID=5D5L7FF6ADF9 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=view&itemId=53-88product_id=53-88"
vitenid=EST-10product_id=RP-LI-02" 468 125.17 "http://buttercup-shopping.com/cart.do?action=view&itemId=53-88product_id=53-88"
//buttercup-shopping.com/cart.do?action=view&itemId=53-88product_id=53-88" 468 125.17 "http://buttercup-shopping.com/cart.do?action=view&itemId=53-88product_id=53-88"
action=purchase&id=RP-LI-02" 468 125.17 "http://buttercup-shopping.com/cart.do?action=view&itemId=53-88product_id=53-88"

```


Kinesis Firehose Use Case

When should I use Kinesis Firehose versus other ingestion mechanisms for Splunk?

Supported Kinesis Firehose Data Sources

Here is a list of AWS Services supported by Kinesis Firehose

▶ AWS CloudWatch Logs

- VPC Flow Logs
- AWS Lambda Logs

▶ CloudWatch Events

- AWS API Call Events (CloudTrail), Auto Scaling Events, AWS CodeBuild Events, AWS CodeCommit Events, AWS CodeDeploy Events, AWS CodePipeline Events, AWS Console Sign-in Events, Amazon EBS Events, Amazon EC2 Events, Amazon EC2 System Manager Events, Amazon EC2 System Manager Configuration Compliance Events, Amazon EC2 Maintenance Window Events, Amazon ECS Events, Amazon EMR Events, Amazon GameLift Event, AWS Health Events, AWS KMS Events, Amazon Macie Events, Scheduled Events, Trusted Advisor Events

▶ AWS IoT

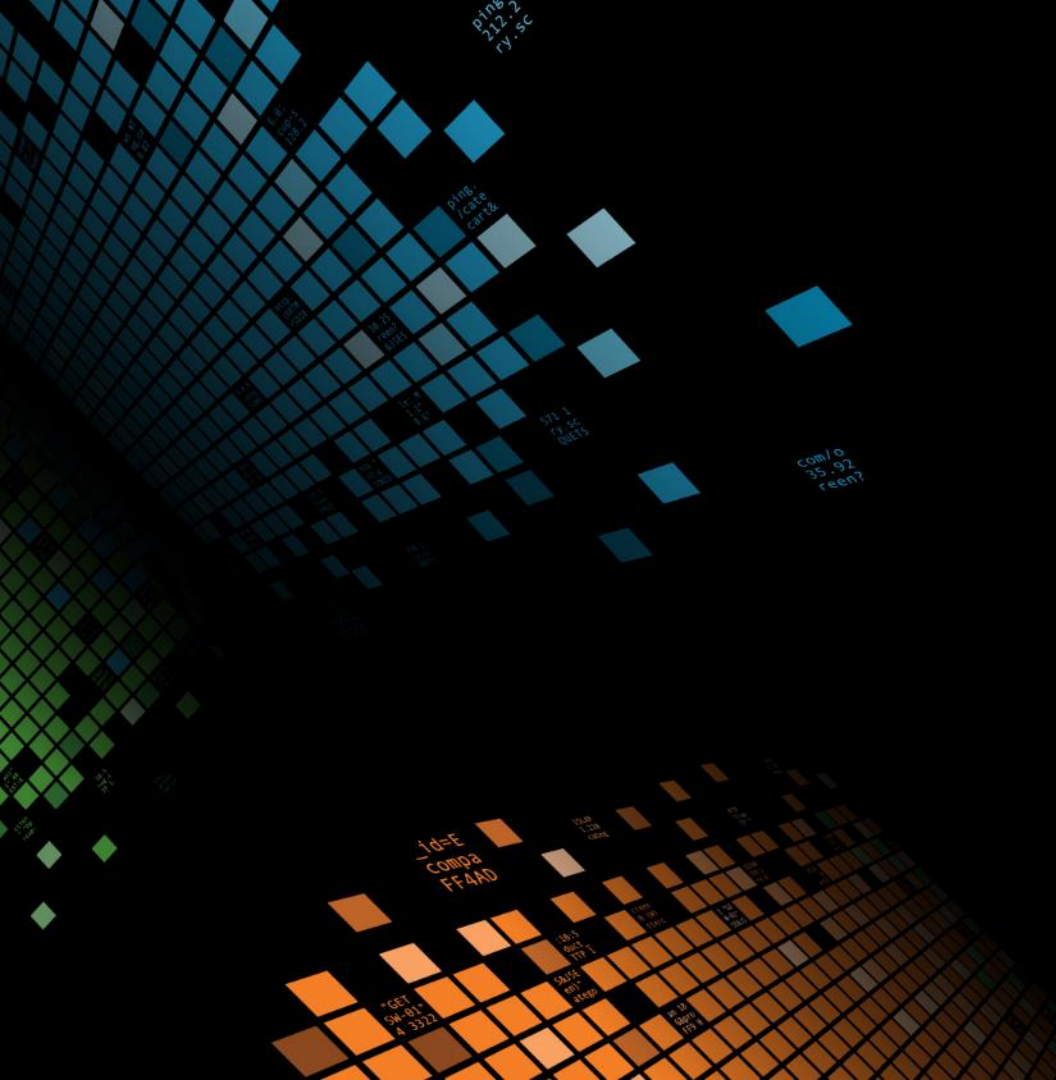
▶ Kinesis Streams

What Ingestion Mechanism Shall I Use?

Use Case	Kinesis Firehose	Splunk AWS Add-on
Supported Kinesis Firehose Data Sources	Preferred	-
Fault tolerance	Yes	Only SQS based S3 input
Guaranteed delivery and reliability	Yes	No
S3 Input	No	Yes
On-Prem Splunk with private IPs	No	Yes
Poll-based Data Collection (Firewall restrictions)	No	Yes

Kinesis Firehose Limits

- ▶ 20 Kinesis Firehose delivery streams per Region
- ▶ Default a maximum of 2,000 transactions/second, 5,000 records/second, and 5 MB/second
- ▶ Limits can be increased, but be careful not to increase past the incoming traffic amount. This can lead to small delivery batches to destinations, which is inefficient and can be costly.
- ▶ Please refer to the Kinesis Firehose documentation for instructions on how to increase limits: <http://docs.aws.amazon.com/firehose/latest/dev/limits.html>



Demo

In Summary

Splunk + AWS = Cloud Visibility

- Strong partnership with numerous product integrations

Current GDI for AWS data into Splunk

- HTTP Event Collector, AWS Add-on, DB Connect

Firehose Kinesis integration

- Addresses scalability and reliability concerns

Q&A

Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk >

.conf2017