



splunk>

# AWS Capacity Planning & Cost Management

Ahmed Kira – Staff Sales Engineer, Splunk

October 2018



# 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. © 2018 Splunk Inc. All rights reserved.

# #whoami

## AHMED KIRA

**AWS SME, Staff SE @ Splunk**

- Creator of AWS for Splunk YouTube videos  
<http://bit.ly/AhmedAWSVideos>
- 3 ½ years at Splunk
- 20+ years in IT
- Network & Systems Engineer by trade



# Agenda

## What will be covered?

1. AWS challenges
2. Addressing these challenges with Splunk
  - End result dashboards & reports
  - Important data sources
  - Architecture
3. Customer Successes

# Customer Challenge



# The Reality



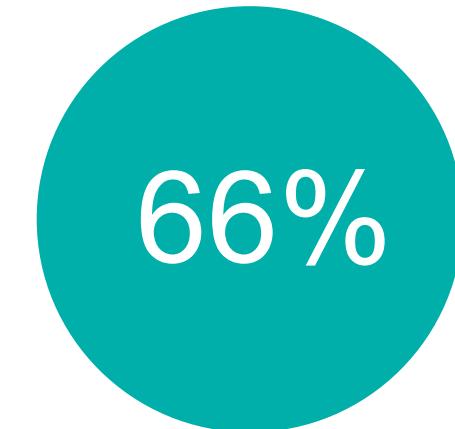
# ...is AWSome.

- ▶ Offers many services & features (3479+)\*
  - ▶ Available across many regions and availability zones
  - ▶ Customers typically have hybrid services (partly in a data center, partly in AWS, partly from other cloud service providers)

\* As of 1 July 2017

# AWS Customer Challenges

- ▶ Controlling AWS costs
- ▶ Track AWS infrastructure and service usage
- ▶ Capacity planning
- ▶ Security of applications and infrastructure



Customers acknowledging 'significant' problems managing AWS spend



Customers admitting AWS spend did not align to their predicted service consumption

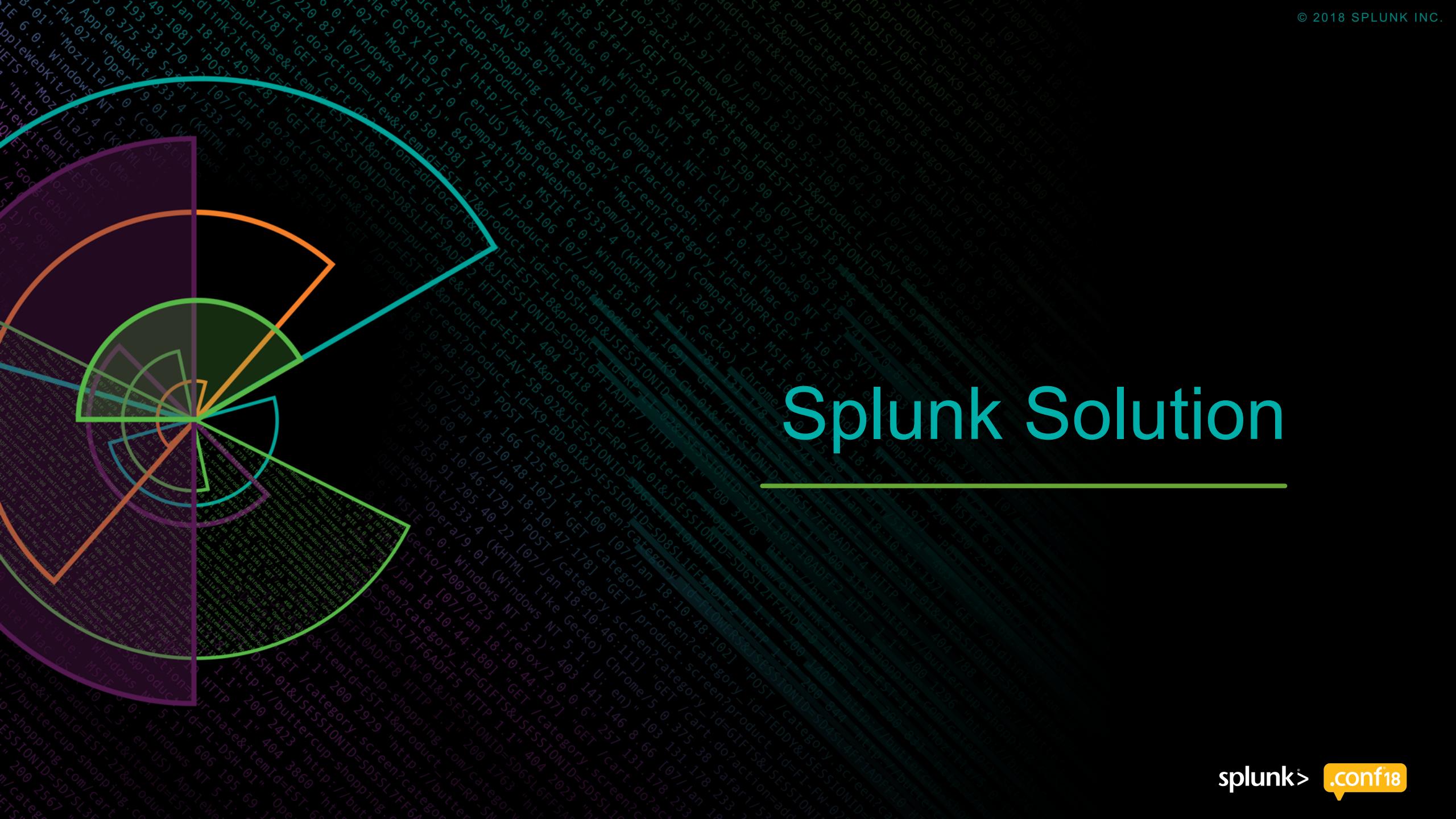
Reference: <https://www.hosting.com/aws-cost-management-challenges/>

<https://www.cloudcruiser.com/press/survey-points-challenges-amazon-web-services-cloud-consumption-cost-controls-allocations/>

# The Challenge... Amplified!

- ▶ Controlling AWS costs
  - ▶ Track AWS infrastructure and service usage
  - ▶ Capacity planning
  - ▶ Security of applications and infrastructure
  - ▶ **Organizations with multiple accounts**
  - ▶ **Services and infrastructure deployed in many AWS Regions and Availability Zones**
  - ▶ **Data taking on many different formats**

# Splunk Solution



# Visualization of AWS data

with

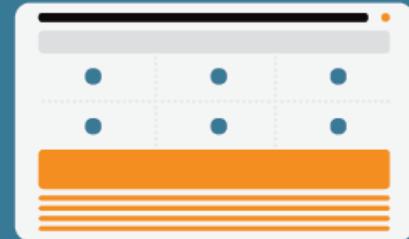
## Splunk App for AWS

### ONE APP

The Splunk App  
for AWS provides countless  
possibilities for operational  
and security visibility.

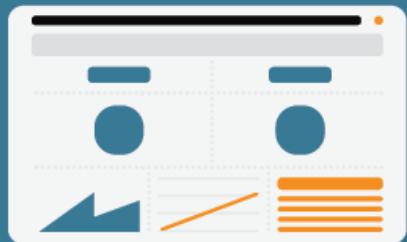


### SECURITY



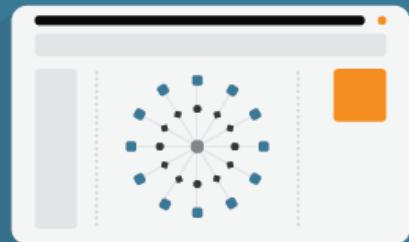
- ✓ Monitor all user & resource activity
- ✓ Get a full audit trail

### COST MANAGEMENT



- ✓ Gain real-time visibility & accountability
- ✓ FINRA saves over 50% on select AWS workloads

### OPERATIONS



- ✓ See and interact with your AWS topology
- ✓ Monitor metrics & VPC traffic

# Data Collection with Splunk Add-on for AWS and/or HTTP Event Collector (HEC)



*End-To-End Visibility*

AWS Cloudtrail

AWS Config

AWS Config Rules

Amazon Inspector

Amazon RDS

Amazon Cloudwatch

Amazon VPC Flow Logs

Amazon S3

Amazon EC2

Amazon CloudFront

Amazon EBS

Amazon ELB

AWS Billing

AWS Personal Health

AWS Lambda

AWS CloudFront

AWS IoT

Amazon GuardDuty

Amazon Macie

Amazon Kinesis Data Firehose

AWS Lambda Serverless Apps

Splunk can ingest, analyze and correlate data from  
**50+ AWS data sources and services**

\* Add-on is leveraged for Capacity Management & Billing data

# Splunk App for AWS – Capacity & Cost Mgmt Dashboards

The screenshot displays the Splunk App for AWS interface, specifically focusing on the Capacity & Cost Mgmt Dashboards. The top navigation bar includes tabs for Overview, Topology, Timeline, Usage, Security, Insights, Billing, and Search. The 'Topology' tab is currently selected, highlighted by a blue border. Below the tabs are several sub-navigation panels:

- Overview:** Includes links for Overview, Usage Overview, Security Overview, Insights Overview, and Anomaly Detection Overview.
- Topology:** Shows a network diagram with nodes representing VPC, Instance, Subnet, Volume, Load Balancer, Security Group, Network Interface, ACL, and Route Table resources. A search bar at the top of this panel allows searching by ID or name.
- Timeline:** Shows a timeline view with various AWS services listed as items.
- Usage:** Shows usage statistics for EC2 Instances, EBS Volumes, ELB Instances, Relational Database Service, Lambda, API Gateway, Capacity Planner, Reserved Instance Planner, and Reserved Instance Inventory.
- Security:** Shows security-related activity for Network ACLs, Security Groups, IAM Activity, Key Pairs Activity, S3 - Data Event, VPC Activity, Resource Activity, User Activity, CloudFront - Traffic Analysis, ELB - Traffic Analysis, S3 - Traffic Analysis, VPC Flow Logs - Traffic Analysis, and VPC Flow Logs - Security Analysis.
- Insights:** Shows insights for EC2, ELB, EBS, and Elastic IP.
- Billing:** Shows budget planning and historical monthly bills.
- Search:** Provides a search interface for navigating through the app's content.

---

## Fun fact



#1

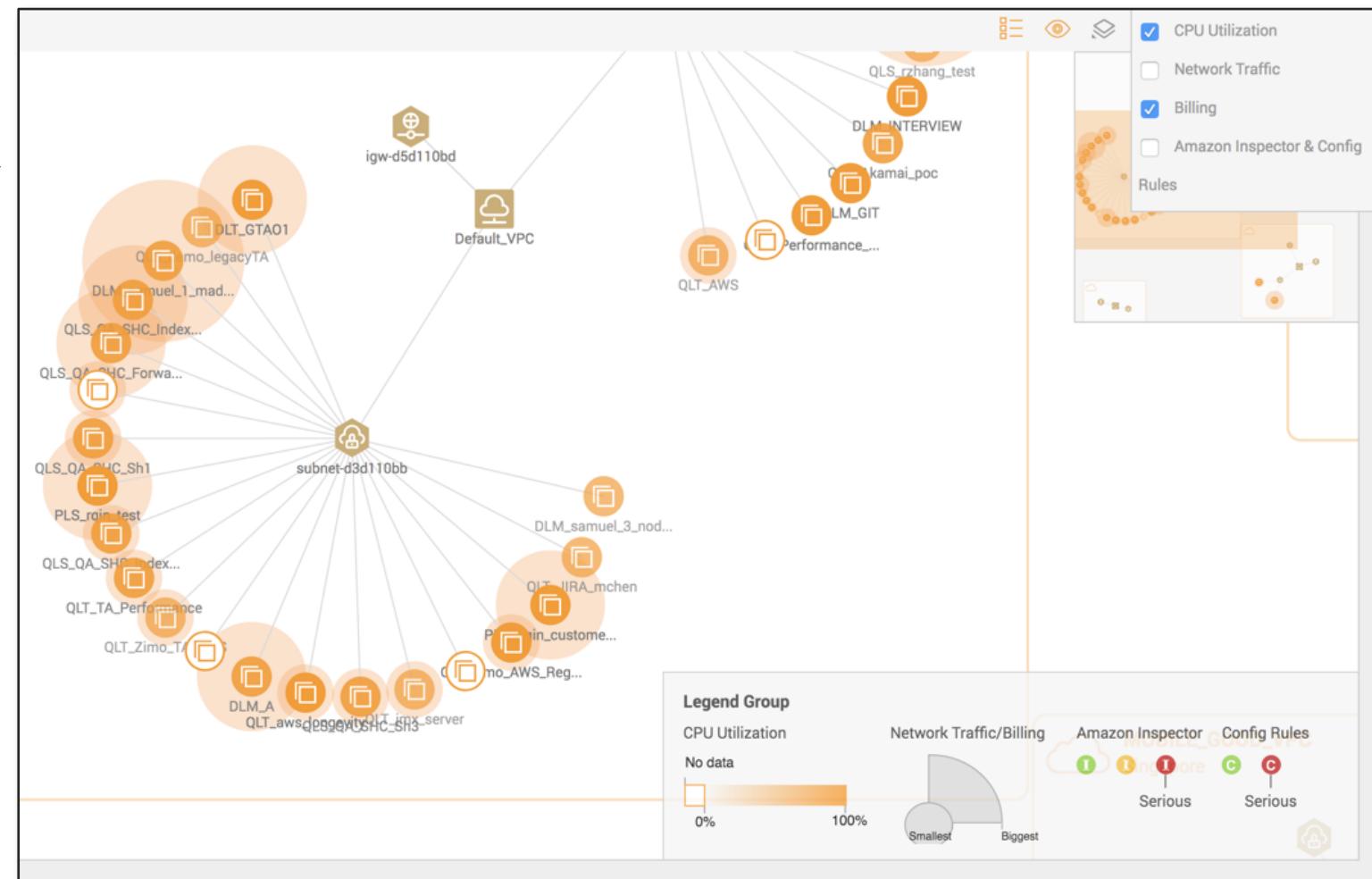
*AWS Billing Reports  
are the  
most accessed  
in the  
Splunk App for AWS  
Amongst Splunk Cloud  
customers*

# Splunk App for AWS – Topology View

Topology can be overlaid with:

- ▶ Resource Cost indicator
- ▶ Resource usage indicator

Visually understand high-cost and over-utilized instances



# Splunk App for AWS – Reserved Instance Planner

Is there a cost savings to convert from on-demand to reserved instances?

Reserved Instance Planner

Account ID 123456789 (IT)	Region All	Platform All	Tenancy All
Instance type All	Basis for insight Prediction	Payment option (one-year term) All upfront	
	History	All upfront	All
	Prediction	Partial upfront	dedicated
		No upfront	default

*i* To keep the prices of EC2 instances up-to-date, use this search command: "|r irecommendation info".

*i* To keep the prices of EC2 instances up-to-date, use this search command: "|r irecommendation info".

! Some panels may not be displayed correctly because the following inputs have not been configured: Billing, Description. Or, the saved search "Addon Metadata - Summarize AWS Inputs" is not enabled on Add-on instance. [Learn more](#)

[Hide Messages](#)

i	Account ID	Region	Platform	Tenancy	Instance type	Existing RIs	Optimal RIs	Estimated yearly savings	Details
>	123456789	China (Beijing)	Linux/UNIX	default	m3	0 (unit)	138 (unit)	¥319,338	<a href="#">Details</a>
>	123456789	China (Beijing)	Linux/UNIX	default	m4	0 (unit)	148 (unit)	¥261,204	<a href="#">Details</a>
▼	123456789	Asia Pacific (Singapore)	Linux/UNIX	default	d2	0 (unit)	240 (unit)	\$107,808	<a href="#">Details</a>
<b>Existing RIs:</b> You already had 0 reserved instance in this category, converting to unit : 0.									
<b>Optimal RIs:</b> Optimal reserved instances are 240 in unit without considering existing ones. With instance size flexibility, any combination of instance type from the d2 family can get your RI benefit. For example: <ul style="list-style-type: none"> <li>• 240 = 240 x 1 (small)</li> </ul>									
>	123456789	EU (Frankfurt)	Linux/UNIX	default	d2	0 (unit)	240 (unit)	\$95,275	<a href="#">Details</a>
>	123456789	Asia Pacific (Sydney)	Linux/UNIX	default	d2	0 (unit)	120 (unit)	\$53,944	<a href="#">Details</a>

# Splunk App for AWS – Budget Planner

Budget Planner

Data Source: Monthly Billing | Account ID: 063605715280 | From: 2018-03 | To: 2018-12 | Monthly Budget: 15000 | Submit

Total Budget: **150,000** | Monthly Budget: **15,000** | Remaining Total Budget: **-35,230,218**

**Budget Burndown**

The chart displays monthly costs (blue bars) and the remaining budget (red line) over time. The x-axis shows months from March 2018 to November. The y-axis ranges from -25,000,000 to 25,000,000. Costs generally increase over time, while the remaining budget decreases sharply, reaching approximately -35,230,218 by July.

Month	Cost	Remaining Budget
March 2018	~500k	~150k
May	~100k	~-100k
July	~150k	~-35,230,218

**Budget**

The chart displays monthly costs (blue bars), budget (green line), and remaining monthly budget (purple line) over time. The x-axis shows months from March 2018 to November. The budget is constant at 15,000. Costs fluctuate, and the remaining monthly budget drops to zero by July.

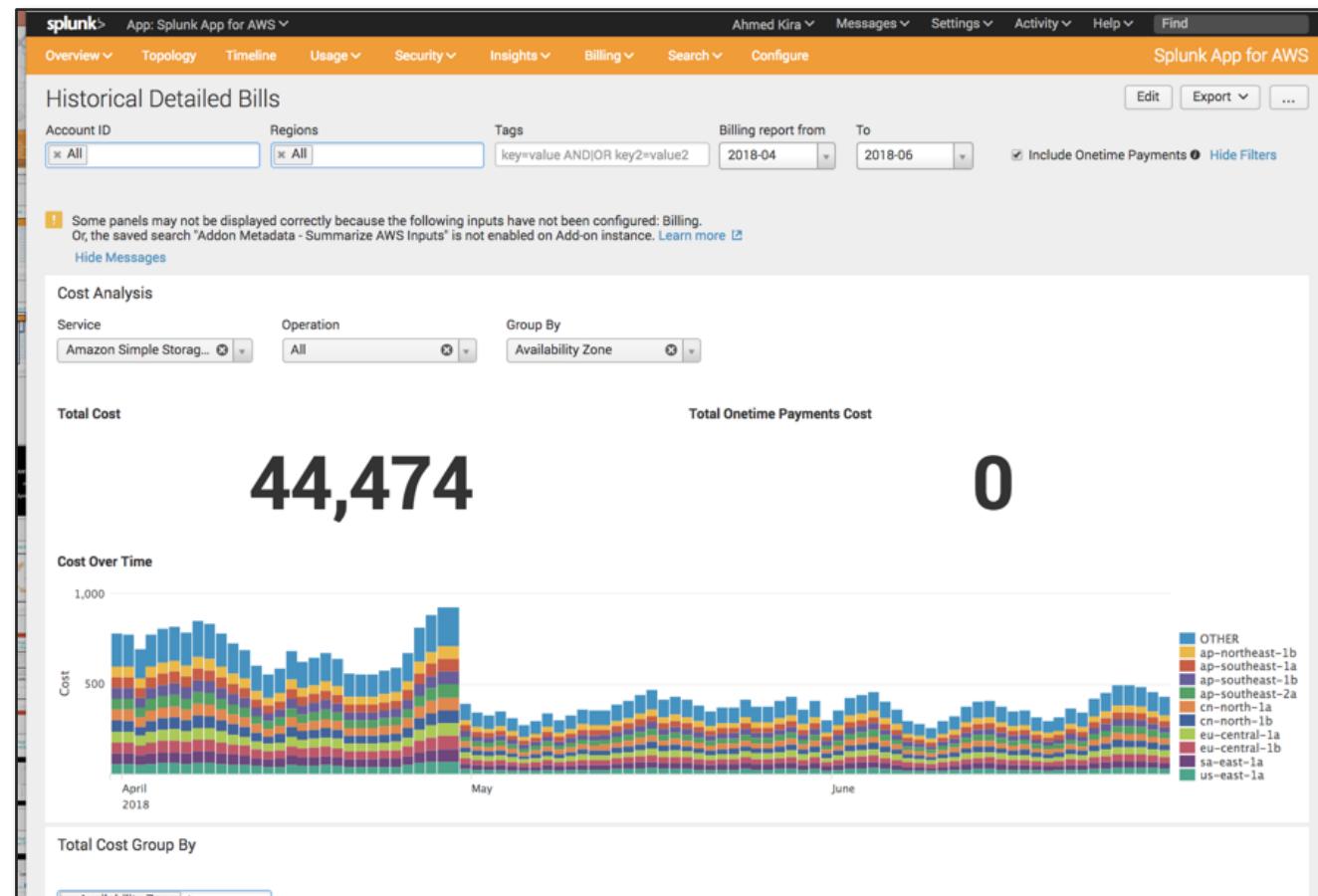
Month	Cost	Budget	Remaining Monthly Budget
March 2018	~500k	15,000	15,000
May	~100k	15,000	15,000
July	~150k	15,000	0

**Month-over-month Budget**

Month	Cost	Balance	Accumulated Cost	Accumulated Balance
2018-03	6,128,136	-6,113,136	6,128,136	-6,113,136
2018-04	2,476,167	-2,461,167	8,604,303	-8,574,303

- ▶ Plan future budgets
- ▶ Identify high-cost services & areas for cost optimization

# Splunk App for AWS – Detailed Billing

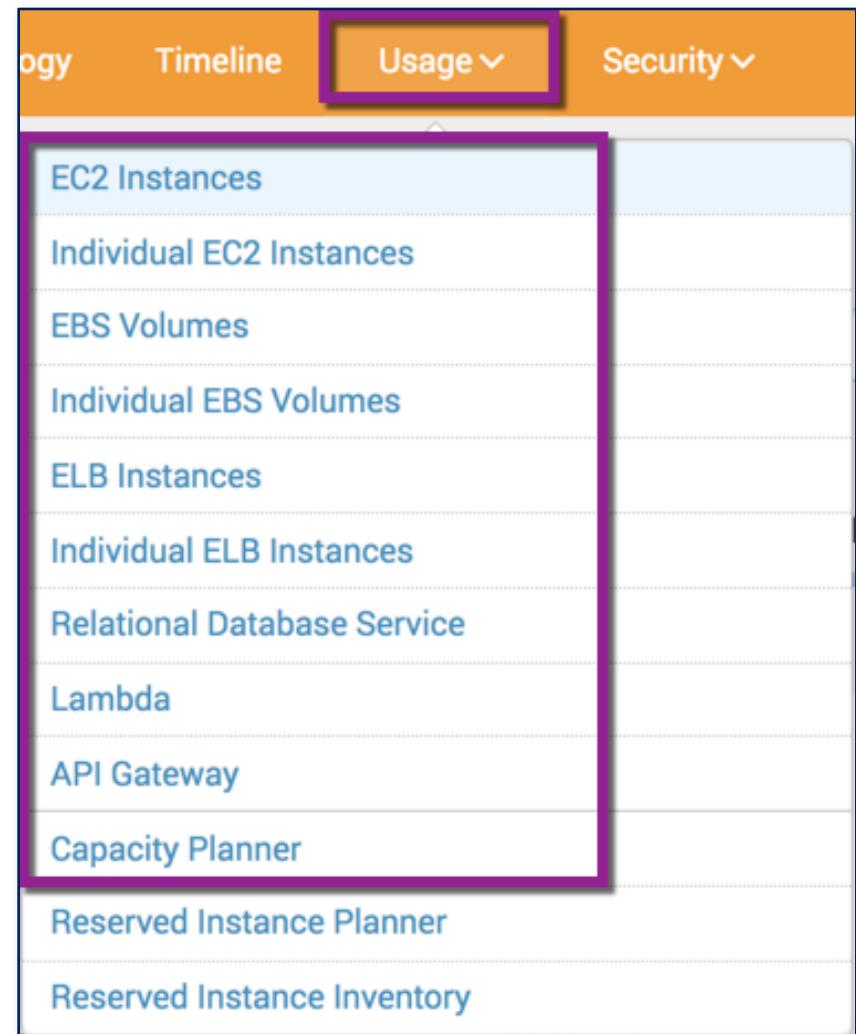


- ▶ Filter to specific services
- ▶ Understand breakdown by operation, region, tag, etc.

# Capacity Planning Dashboards

Section subtitle goes here

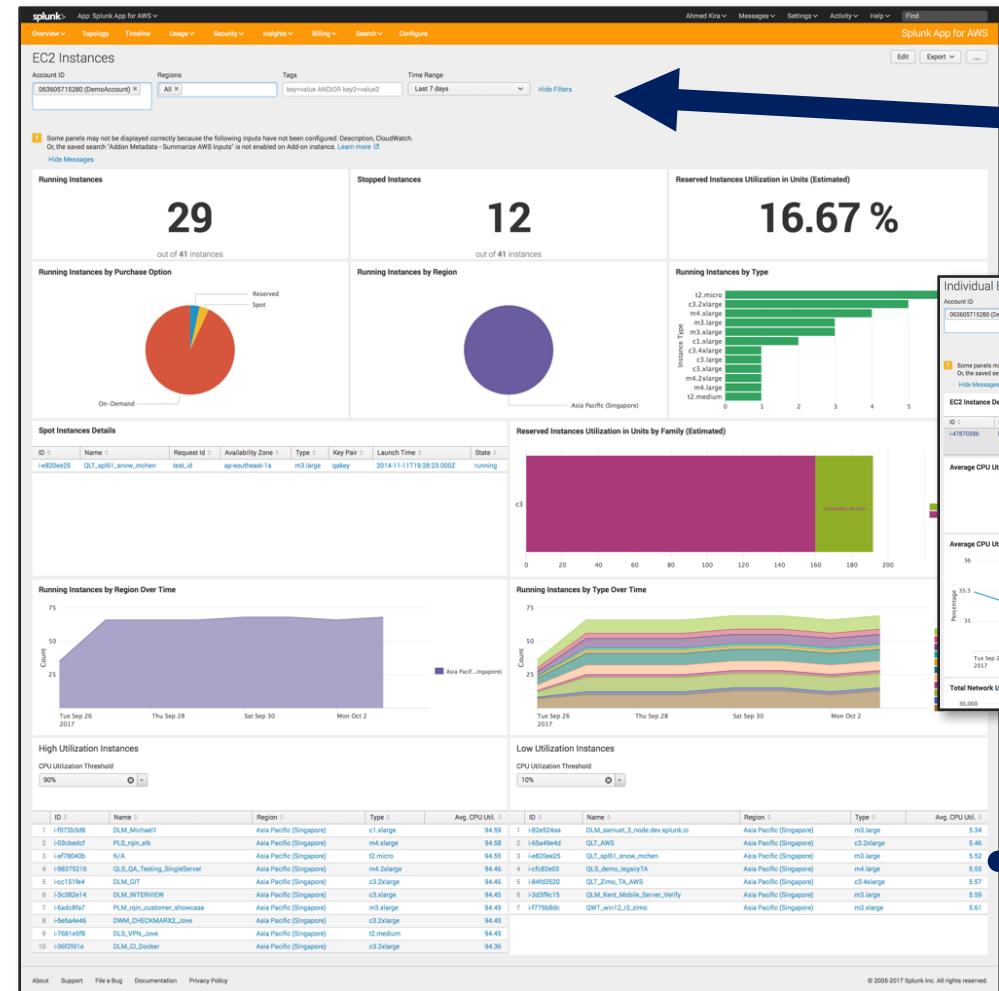
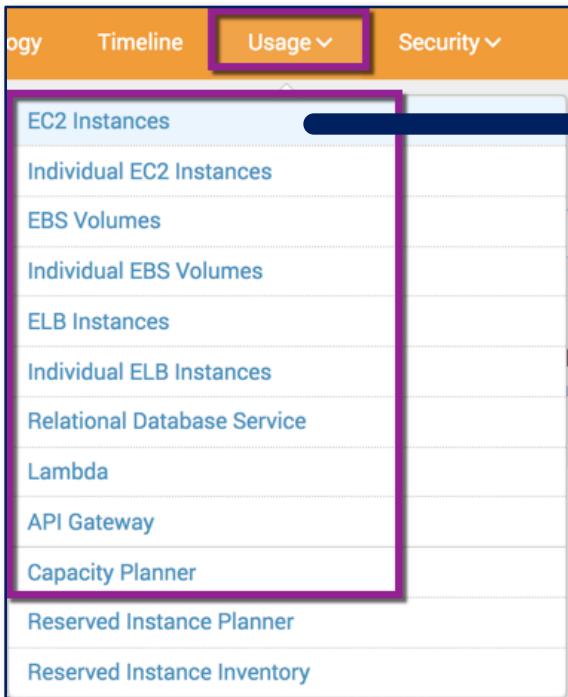
# Capacity Management Relevant Views



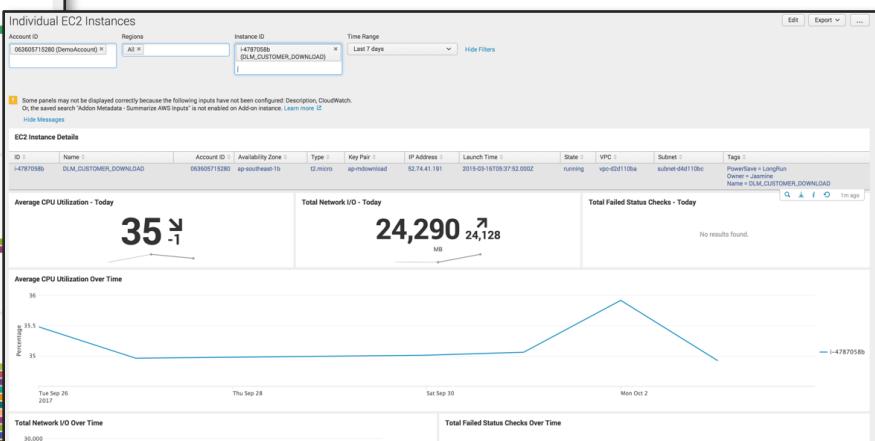
Out of box dashboards for popular AWS Services

Can be leveraged as templates for custom dashboards

# What EC2 instances are over or under utilized?

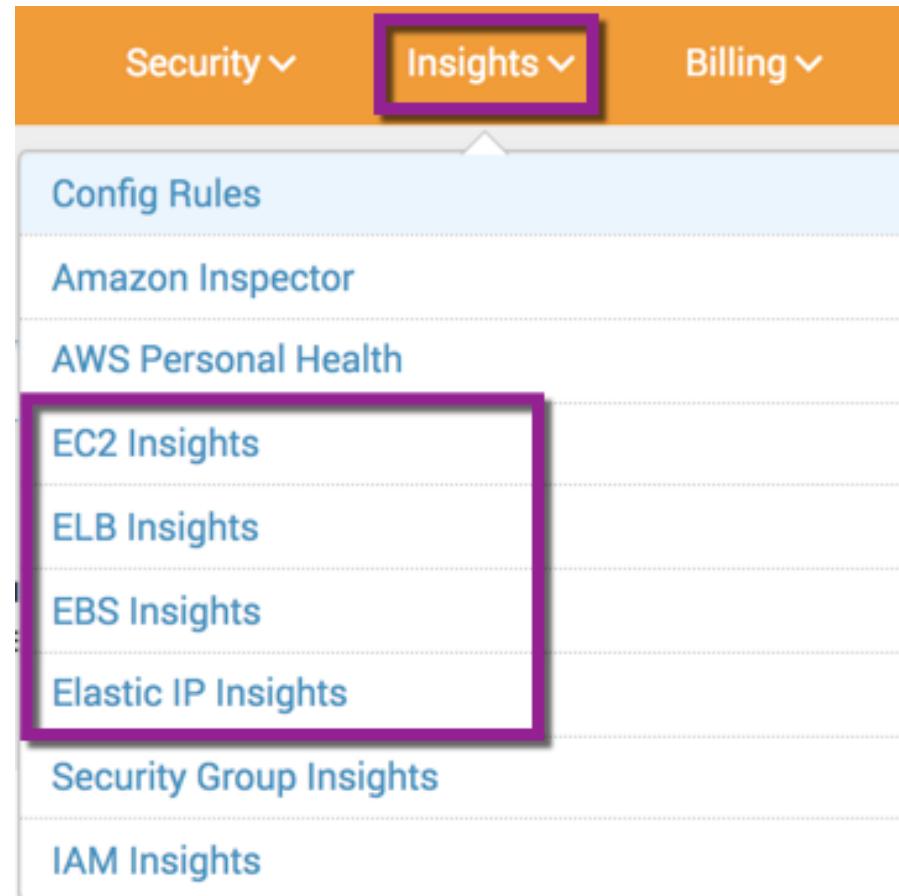


Filter by Account, Region, Tag



Drill into under-utilized or over-utilized instance details

# Insights dashboards



What EBS volumes are unused?

What ec2 instances need to be upgraded?

What ec2 instances need to be downgraded?

What load balancer is unhealthy?

What load balancer sessions are insecure?

What is not cross-zone for high availability?

# Splunk App for AWS EC2 instance insights

**EC2 Insights**

Account ID Regions Instance Type Tags

key=value AND/OR key2=value2  
AWSTesting  
Application  
Description  
Installed  
Name  
Owner  
PowerSave  
Provisioner

Hide Filters

Insights on this dashboard are based on CloudWatch data from the past week and require at least 2 days worth of data to be available.

Some panels may not be displayed correctly because the following inputs have not been configured: Description, CloudWatch Metrics, or the saved search "Addon Metadata - Summarize AWS Inputs" is not enabled on Add-on instance. [Learn more](#)

Hide Messages

i	Account	Instance ID	Instance Name	Region	Action	
>	063	i-f775b8dc	QWT_win12_r2_zimo	m3.xlarge	ap-southeast-1	Downgrade
>	063	i-e820ee25	QLT_spl61_snow_mchen	m3.large	ap-southeast-1	Downgrade
>	063	i-0354b028	QLT_spl61_aws_01_mchen	m3.large	ap-southeast-1	Upgrade

Instance i-0354b028 is overutilized. Consider upgrading this instance to improve performance.

To upgrade this instance using the CLI tool, follow the steps below. You can also upgrade this instance using the AWS Management Console. [Learn more](#)

1. Stop your instance.

```
aws ec2 stop-instances --instance-ids i-0354b028 --region ap-southeast-1
```

2. Modify your instance type. In the command below, replace INSTANCE TYPE with the value of the instance type that you want to downgrade to.

```
aws ec2 modify-instance-attribute --instance-id i-0354b028 --region ap-southeast-1 --instance-type {"Value": "INSTANCE TYPE"}
```

3. Start your instance.

```
aws ec2 start-instances --instance-ids i-0354b028 --region ap-southeast-1
```

i	Account	Instance ID	Instance Name	Region	Action	
>	063	i-940013bc	QLT_spl60_aws_mchen	m3.large	ap-southeast-1	Downgrade
>	063	i-1073aed	QLT_jmx_server	m3.xlarge	ap-southeast-1	Downgrade

## Features

- ▶ Determine which instances need to be right-sized
- ▶ Copy/Paste commands to AWS CLI
- ▶ Filter by tag, region, account

## Value Realized

- ▶ Maintain costs without sacrificing performance

# More Insights for popular AWS services

**EBS Insights**

Account ID: 063605 Regions: All Tags: key=value AND/OR key2=value2

Insights Filter: \* All | Unattached EBS, Non-optimized EBS, No Snapshot(30 days), Large IOPS, Small IOPS

Some panels may not be displayed correctly because the following inputs have not been configured: Description, CloudWatch. Or, the saved search "Addon Metadata - Summarize AWS Inputs" is not enabled on Add-on instance. Learn more [\[link\]](#)

Hide Messages

i	ID	Region	Owner	Type	State	Insight	Severity
>	vol-1E	Asia Pacific (Singapore)	PowerSave	standard	in-use	No Recent Snapshot	⚠️
>	vol-2E	Asia Pacific (Singapore)	Provisioner	300	io1	No Recent Snapshot	⚠️
>	vol-7E	Asia Pacific (Singapore)		300	standard	No Recent Snapshot	⚠️
>	vol-2E	Asia Pacific (Singapore)		300	io1	Small IOPS	⚠️
>	vol-f0E	Asia Pacific (Singapore)		250	standard	No Recent Snapshot	⚠️
>	vol-0C	Asia Pacific (Singapore)		200	io1	No Recent Snapshot	⚠️
>	vol-74E	Asia Pacific (Singapore)		200	standard	No Recent Snapshot	⚠️
>	vol-8tE	Asia Pacific (Singapore)		200	standard	No Recent Snapshot	⚠️
>	vol-7E	Asia Pacific (Singapore)		160	gp2	No Recent Snapshot	⚠️
>	vol-a9E	Asia Pacific (Singapore)		100	gp2	available	Unattached
>	vol-b8E	Asia Pacific (Singapore)		100	gp2	available	Unattached

Eliminate unused services

Add capacity for unhealthy Load Balancer or low IOPS volumes

**ELB Insights**

Account ID: 1234567890 Regions: All Insights Filter: \* All | Hide Filters

Some panels may not be displayed correctly because the following inputs have not been configured: Description, CloudWatch. Or, the saved search "Addon Metadata - Summarize AWS Inputs" is not enabled on Add-on instance. Learn more [\[link\]](#)

Hide Messages

i	Account ID	Region	Name	Type	Availability zones	Insight	Severity
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Classic	ap-southeast-1a,ap-southeast-1b	No healthy instance	❗
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1b,ap-southeast-1a	Application	ap-southeast-1b,ap-southeast-1a	No healthy instance	❗
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Classic	ap-southeast-1a,ap-southeast-1b	One healthy instance without autoscaling	⚠️
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Application	ap-southeast-1a,ap-southeast-1b	One healthy instance without autoscaling	⚠️
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Classic	ap-southeast-1a,ap-southeast-1b	Insecure listener protocol	⚠️
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Classic	ap-southeast-1a,ap-southeast-1b	Insecure listener protocol	⚠️
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Classic	ap-southeast-1a,ap-southeast-1b	Insecure listener protocol	⚠️
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1b,ap-southeast-1a	Application	ap-southeast-1b,ap-southeast-1a	Insecure listener protocol	⚠️
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Classic	ap-southeast-1a,ap-southeast-1b	Healthy instances are not cross-zone	⚠️
>	1234567890	Asia Pacific (Singapore)	ap-southeast-1a,ap-southeast-1b	Application	ap-southeast-1a,ap-southeast-1b	Healthy instances are not cross-zone	⚠️

**Elastic IP Insights**

Account ID: All Regions: All Insights Filter: \* All | Hide Filters

Some panels may not be displayed correctly because the following inputs have not been configured: Description. Or, the saved search "Addon Metadata - Summarize AWS Inputs" is not enabled on Add-on instance. Learn more [\[link\]](#)

Hide Messages

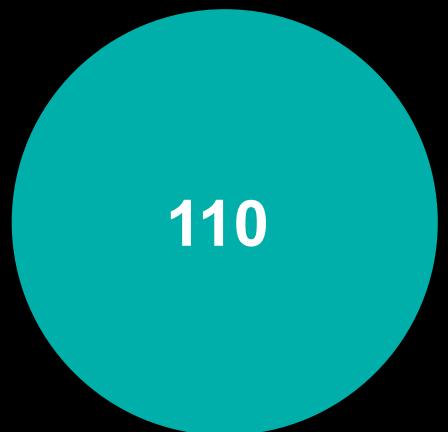
i	Account ID	Region	Public IP	Attached Instance	Insight	Severity
>	All	Asia Pacific (Singapore)	13.228.128.128	N/A	No attached instance	❗
>	All	Asia Pacific (Singapore)	54.169.128.128	i3b05718 (DWM_Good_MDM)	Inactive attached instance	⚠️

# Takeaways on Why Splunk?



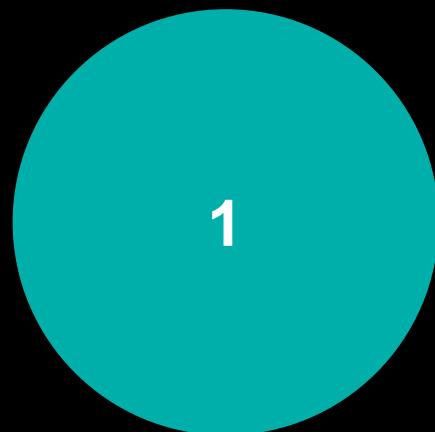
unlimited

Number of accounts you can manage with Splunk App & Add-on for AWS



110

Number of out of box dashboards & reports



1

Location to report & correlate data

138.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=EST-6&product\_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:57:153] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=product&itemId=EST-26&product\_id=EST-26&product\_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=oldlink?item\_id=EST-18&product\_id=EST-18&product\_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:55:187] "GET /oldlink?item\_id=EST-68&JSESSIONID=SD10SLBFF2ADFF9 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=oldlink?item\_id=EST-68&product\_id=EST-68&product\_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:55:187] "GET /category.screen?category\_id=SURPRISE&JSESSIONID=SD85L8FF1ADFF4 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product\_id=EST-10&product\_name=Buttercup Shopping" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

# How is it done?



# It's all about the right data



## Main Data Sources:

- ▶ AWS CloudWatch metrics
    - All AWS Services (Lambda, ec2, EBS, Kinesis, etc.)
    - Billing summary metrics
  - ▶ AWS Billing Reports
    - ‘Cost & Usage’
    - ‘Monthly’
    - ‘Monthly Cost Allocation’
    - ‘Detailed Billing’
    - ‘Detailed Billing w/resources & tags’

# CloudWatch metrics



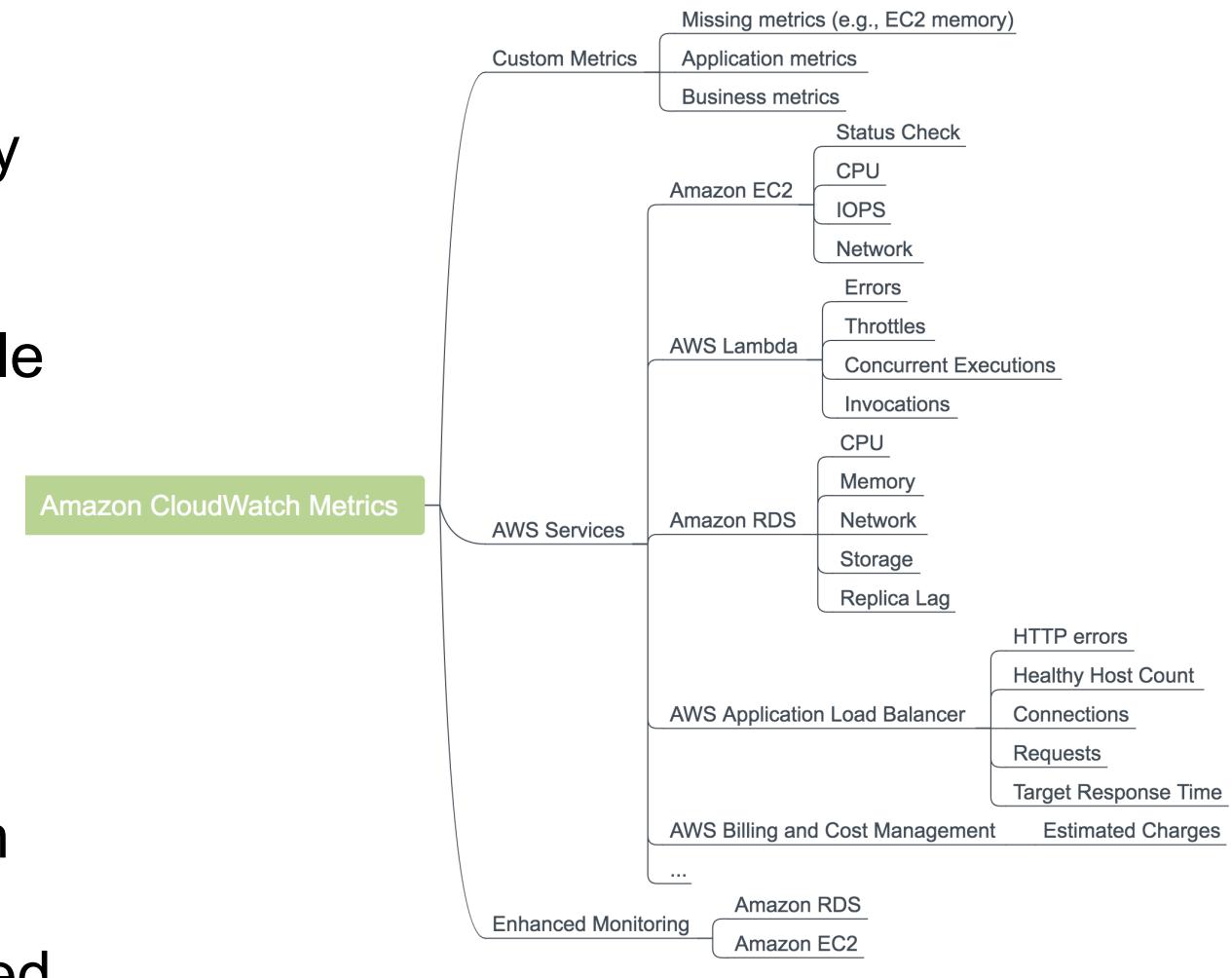
# AWS CloudWatch Metrics

AWS collects metrics for virtually all enabled services

Estimated Charges also available as CloudWatch Metrics

CloudWatch metrics in Splunk help:

- ▶ Predict future resource utilization
- ▶ Correlate resource usage with transaction activity
- ▶ Locate unused or under-utilized resources



Reference: <https://cloudonaut.io/aws-monitoring-primer/>

# AWS Permissions for CloudWatch Metrics

- ▶ Add these permissions to a policy
- ▶ Assign policy to either:
  - ec2 instance role
  - Account & user (i.e. awssplunkaccount/root, myaccount/splunkuser)

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

Documentation:

[https://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSPermissions#Configure\\_CloudWatch\\_permissions](https://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSPermissions#Configure_CloudWatch_permissions)

# CloudWatch Input within Splunk Add-on for AWS

- ▶ Enhanced in Add-on version 4.4+.
- ▶ Many default metrics pre-defined
- ▶ Option to select advanced mode for additional metrics

Notice  
AWS/Billing is  
enabled by  
default

**AWS Input Configuration** Learn more ↗

Name	<input type="text"/>
AWS Account	<input type="button" value="Select a value"/>
Assume Role	<input type="button" value="optional"/>
AWS Regions	<input type="text"/>

---

**Metrics Configuration** (Edit in advanced mode)

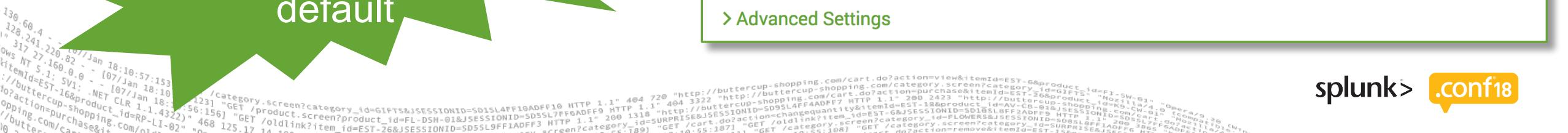
Name Service (9)	Dimensions	Metrics
AWS/ApiGateway	All	All
AWS/ApplicationELB	All	All
AWS/Billing	All	All
AWS/EBS	All	All
AWS/EC2	All	All
AWS/ELB	All	All
AWS/Lambda	All	All
AWS/RDS	All	All
AWS/S3	All	All

---

**Splunk-related Configuration**

Source Type	<input type="text" value="aws:cloudwatch"/>
Index	<input type="button" value="default"/>

[» Advanced Settings](#)



# What about CloudWatch metrics from other namespaces?

Simplified setup  
for enabling  
additional  
CloudWatch  
metrics

Metrics Configuration [\(Edit in advanced mode\)](#)

Namespace

- AWS/ApiGateway
- AWS/ApplicationELB
- AWS/Billing
- AWS/EBS
- AWS/EC2
- AWS/ELB
- AWS/Lambda
- AWS/RDS
- AWS/S3
- AWS/AutoScaling**
- AWS/CloudFront
- AWS/CloudSearch
- AWS/DX
- AWS/DynamoDB
- AWS/ECSSpot
- AWS/ECS
- AWS/ES
- AWS/ElastiCache
- AWS/ElasticMapReduce
- AWS/Events
- AWS/Kinesis
- AWS/Logs

+ Add Namespace

All

Metrics

- GroupDesiredCapacity
- GroupInServiceInstances
- GroupMaxSize
- GroupMinSize
- GroupPendingInstances
- GroupStandbyInstances
- GroupTerminatingInstances
- GroupTotalInstances

Dimension	Dimension Value ?	Metrics	Metric Statistics
AutoScalingGroupName	[{"AutoScalingGroupName": "*"}]	x All	<input checked="" type="checkbox"/> Average <input type="checkbox"/> Sum <input type="checkbox"/> SampleCount <input type="checkbox"/> Maximum <input type="checkbox"/> Minimum

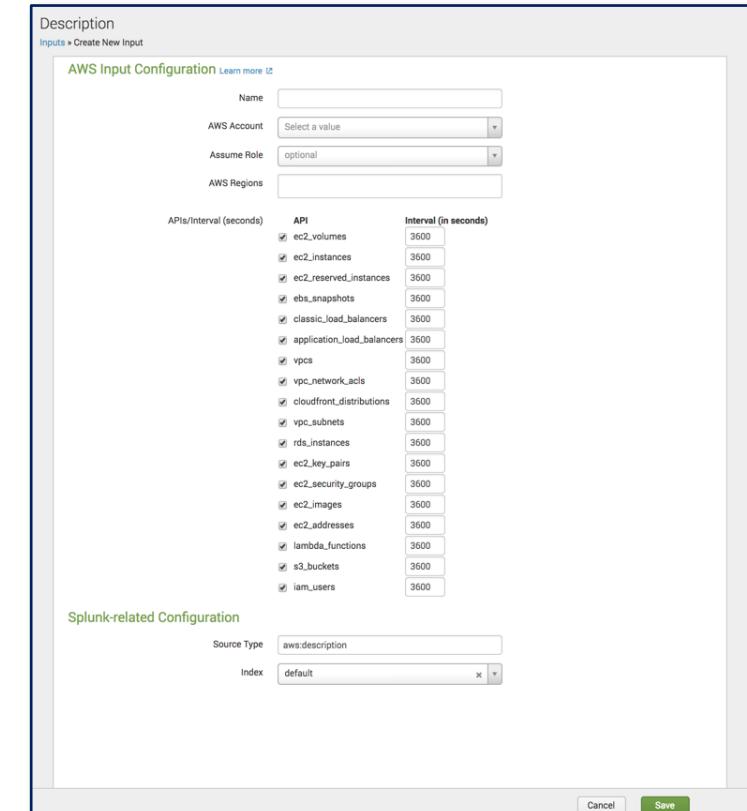
# Required Description Input & Permissions

Description input required for AWS App Dashboard charts

Apply these AWS permissions to your account or ec2 instance role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeRegions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAddresses",
        "lambda>ListFunctions",
        "rds:DescribeDBInstances",
        "cloudfront>ListDistributions",
        "iam: GetUser",
        "iam: ListUsers",
        "iam: GetAccountPasswordPolicy",
        "iam: ListAccessKeys",
        "iam: GetAccessKeyLastUsed",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "s3:ListAllMyBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketCORS",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketTagging"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```
"iam: GetUser",
"iam: ListUsers",
"iam: GetAccountPasswordPolicy",
"iam: ListAccessKeys",
"iam: GetAccessKeyLastUsed",
"elasticloadbalancing: DescribeLoadBalancers",
"elasticloadbalancing: DescribeInstanceHealth",
"elasticloadbalancing: DescribeTags",
"elasticloadbalancing: DescribeTargetGroups",
"elasticloadbalancing: DescribeTargetHealth",
"elasticloadbalancing: DescribeListeners",
"s3: ListAllMyBuckets",
"s3: GetAccelerateConfiguration",
"s3: GetBucketCORS",
"s3: GetLifecycleConfiguration",
"s3: GetBucketLocation",
"s3: GetBucketLogging",
"s3: GetBucketTagging"
```



# Billing Reports

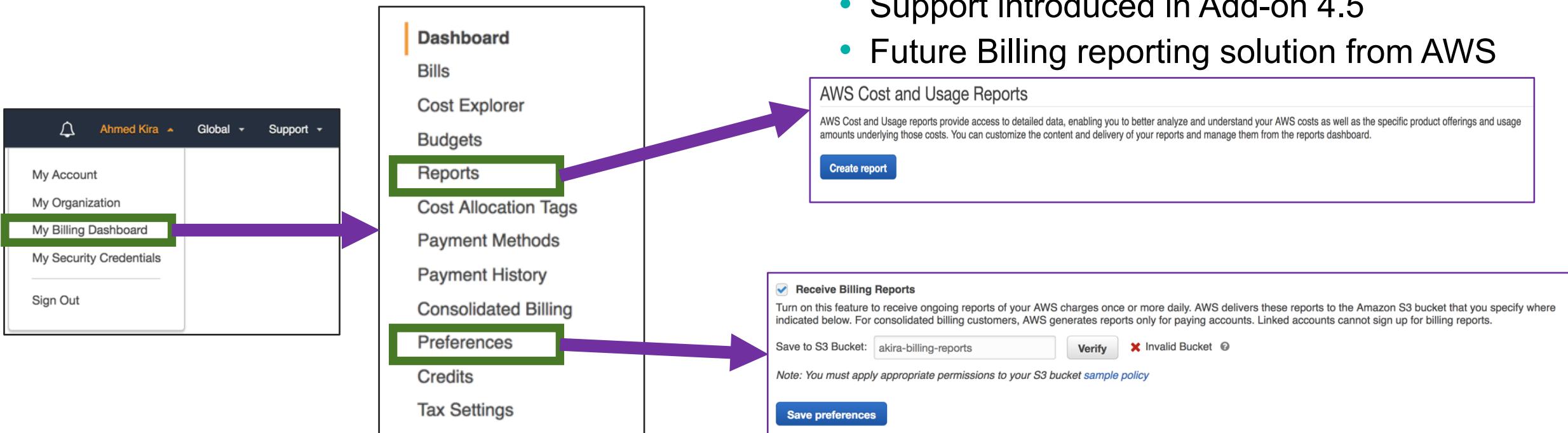
# Relevant AWS Billing Data

Data Source	Ingest Method	Collection Interval	Sourcetypes / Event Types	Reports / Dashboards
Monthly Report	Billing Input (read through API)	Daily Snapshot (Month to Date Totals)	Sourcetype: aws:billing Eventtype: aws_billing_monthly_report	“Total” or “monthly” reports & dashboards
Monthly Cost Allocation Report	Billing Input (read from an S3 bucket)	Daily Snapshot (Month to Date Totals)	Sourcetype: aws:billing Eventtype: aws_billing_monthly_report	“Total” or “monthly” reports & dashboards
Detailed Billing Report	Billing Input (read from an S3 bucket)	Monthly Collection (followed by daily collection until finalized)	Sourcetype: aws:billing Eventtype: aws_billing_detail_report	“Daily” reports & dashboards
Detail Billing Report with resource & tags	Billing Input (read from an S3 bucket)	Monthly Collection (followed by daily collection until finalized)	Sourcetype: aws:billing Eventtype: aws_billing_detail_report	“Daily” reports & dashboards
CloudWatch Billing Metrics	CloudWatch Input	Configurable in seconds (i.e. 60 seconds, 3600 seconds)	Sourcetype: Aws:cloudwatch Eventtype: aws_cloudwatch_billing_events	Current Month Estimated Billing  Budget Planner (option)
Cost & Usage Report	New Billing Input (read from an S3 bucket)	Daily Collection (monthly report w/ MTD totals)	Sourcetype: aws:billing:cur	

# Recommended reports to make available for Splunk

Data Source	Ingest Method	Collection Interval	Sourcetypes / Event Types	Reports / Dashboards
Monthly Report	Billing Input (read through API)	Daily Snapshot (Month to Date Totals)	Sourcetype: aws:billing Eventtype: aws_billing_monthly_report	“Total” or “monthly” reports & dashboards
Monthly Cost Allocation Report	Billing Input (read from an S3 bucket)	Daily Snapshot (Month to Date Totals)	Sourcetype: aws:billing Eventtype: aws_billing_monthly_report	“Total” or “monthly” reports & dashboards
Detailed Billing Report	Billing Input (read from an S3 bucket)	Monthly Collection (followed by daily collection until finalized)	Sourcetype: aws:billing Eventtype: aws_billing_detail_report	“Daily” reports & dashboards
Detail Billing Report with resource & tags	Billing Input (read from an S3 bucket)	Monthly Collection (followed by daily collection until finalized)	Sourcetype: aws:billing Eventtype: aws_billing_detail_report	“Daily” reports & dashboards
CloudWatch Billing Metrics	CloudWatch Input	Configurable in seconds (i.e. 60 seconds, 3600 seconds)	Sourcetype: Aws:cloudwatch Eventtype: aws_cloudwatch_billing_events	Current Month Estimated Billing  Budget Planner (option)
Cost & Usage Report	New Billing Input (read from an S3 bucket)	Daily Collection (monthly report w/ MTD totals)	Sourcetype: aws:billing:cur	

# Setting up Billing Reports in AWS Console



## ► ‘Cost & Usage’ report

- Support introduced in Add-on 4.5
- Future Billing reporting solution from AWS

## AWS Cost and Usage Reports

AWS Cost and Usage reports provide access to detailed data, enabling you to better analyze and understand your AWS costs as well as the specific product offerings and usage amounts underlying those costs. You can customize the content and delivery of your reports and manage them from the reports dashboard.

[Create report](#)

### Receive Billing Reports

Turn on this feature to receive ongoing reports of your AWS charges once or more daily. AWS delivers these reports to the Amazon S3 bucket that you specify where indicated below. For consolidated billing customers, AWS generates reports only for paying accounts. Linked accounts cannot sign up for billing reports.

Save to S3 Bucket:

[Verify](#)

Invalid Bucket [?](#)

Note: You must apply appropriate permissions to your S3 bucket [sample policy](#)

[Save preferences](#)

## ► ‘Traditional’ reports

## ► CloudWatch Billing metrics

# Setup AWS Permissions

- ▶ Within S3 bucket in billing master account(s):

- Setup bucket policy to grant read-access to the Splunk Add-on account/role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Billing permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::SplunkAccountNumber:  
-name_of_user(default:root)"
      },
      "Action": [
        "s3:Get*",
        "s3>List*"
      ],
      "Resource": [
        "arn:aws:s3:::BillingReportsBucketARN"
      ]
    }
  ]
}
```

- ▶ Within account/role that Splunk Add-on runs as:

- If policy is defined on master account billing S3 bucket, no additional steps required.
- assumeRole option if a different role has the required permissions

Reference Documentation:

<https://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSPermissions>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html>

# Billing Inputs within Splunk Add-on for AWS

## Traditional Billing Input

**AWS Input Configuration** Learn more ↗

Name	BillingReports-AggregateAccount
AWS Account	Select a value
Assume Role	optional
S3 Bucket	Select a value
Monthly Report	Monthly cost allocation report
Detail Report	Detailed billing report with resources and tags

**Splunk-related Configuration**

Start Date/Time (UTC)	2018-04-01T00:00:00Z
Source Type	aws:billing
Index	default

**Advanced Settings**

Interval (in seconds)	86400
Regex for Report Selection ?	optional
Temp Folder ?	optional

## Cost & Usage Report Input

**AWS Input Configuration** Learn more ↗

Name	CostAndUsageReport_Input
AWS Account	Select a value
Assume Role	optional
S3 Bucket	Select a value
Report Prefix	optional
Report Name Pattern	A regular expression used to filter reports by name

**Splunk-related Configuration**

Start Date	2018-05
Source Type	aws:billing:cur
Index	default

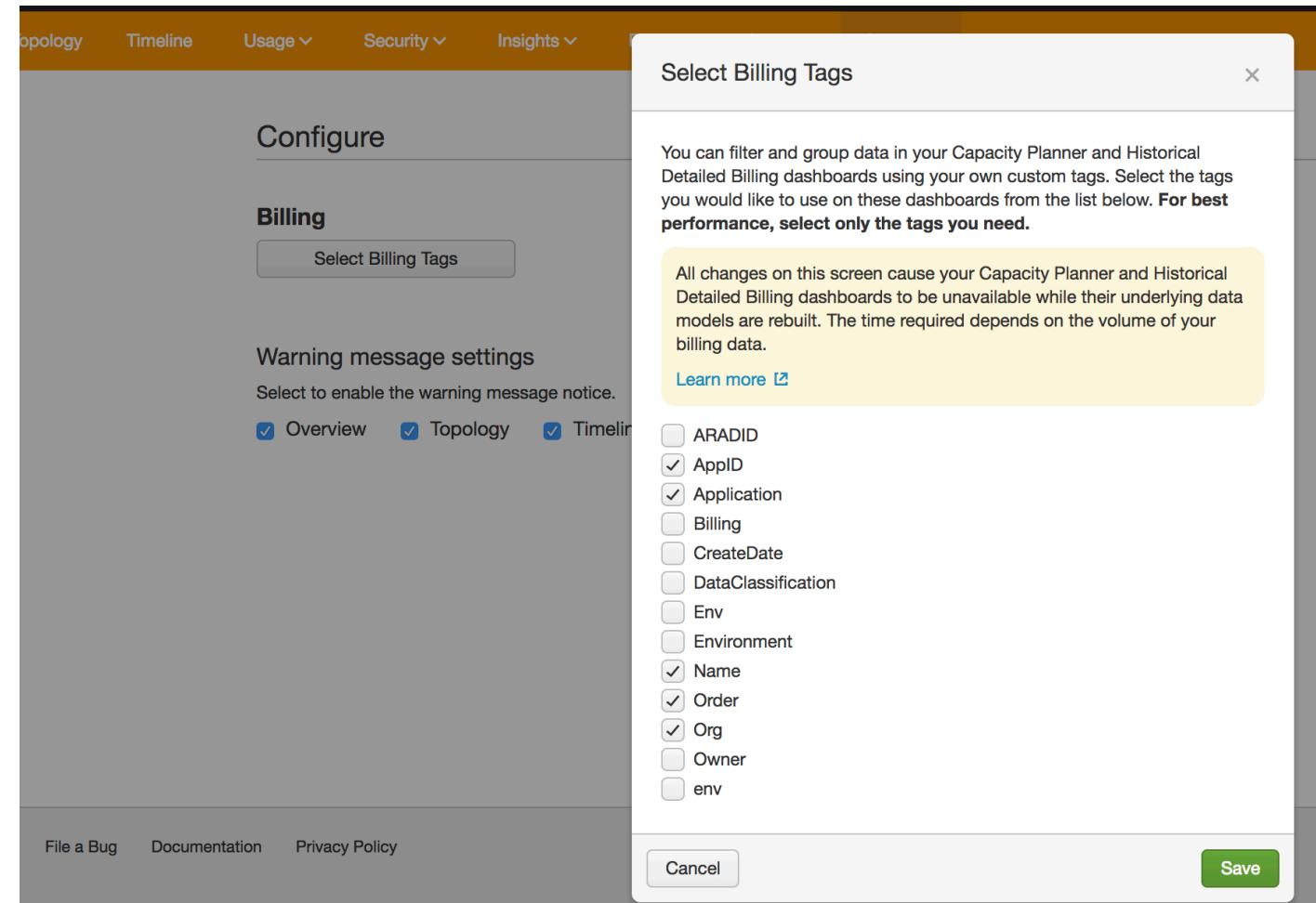
**Advanced Settings**

Interval (in seconds)	3600
Temp Folder ?	optional

# Enabling tag filtering in AWS App Billing Reports

Within AWS App,  
select  
**Configure** menu

'Select Billing Tags'  
should appear after  
billing w/tag data is  
processed (up to 48  
hours after setup)



# Splunk Setup & Considerations

# Want AWS Only Visibility?

# Splunk Insights for AWS Cloud Monitoring

# Setup for max 10 GB/day



# Splunk Insights for AWS Cloud Monitoring PAYG

Sold by: [Splunk Inc.](#)   Latest Version: 7.0.3\*

Available for FREE for a 15-day trial and provides visibility into your AWS infrastructure, delivering real-time awareness of performance, health, configuration, security and

[▼ Show more](#)

Linux/Unix       (0)      [Free Trial](#)

[Continue to Subscribe](#)

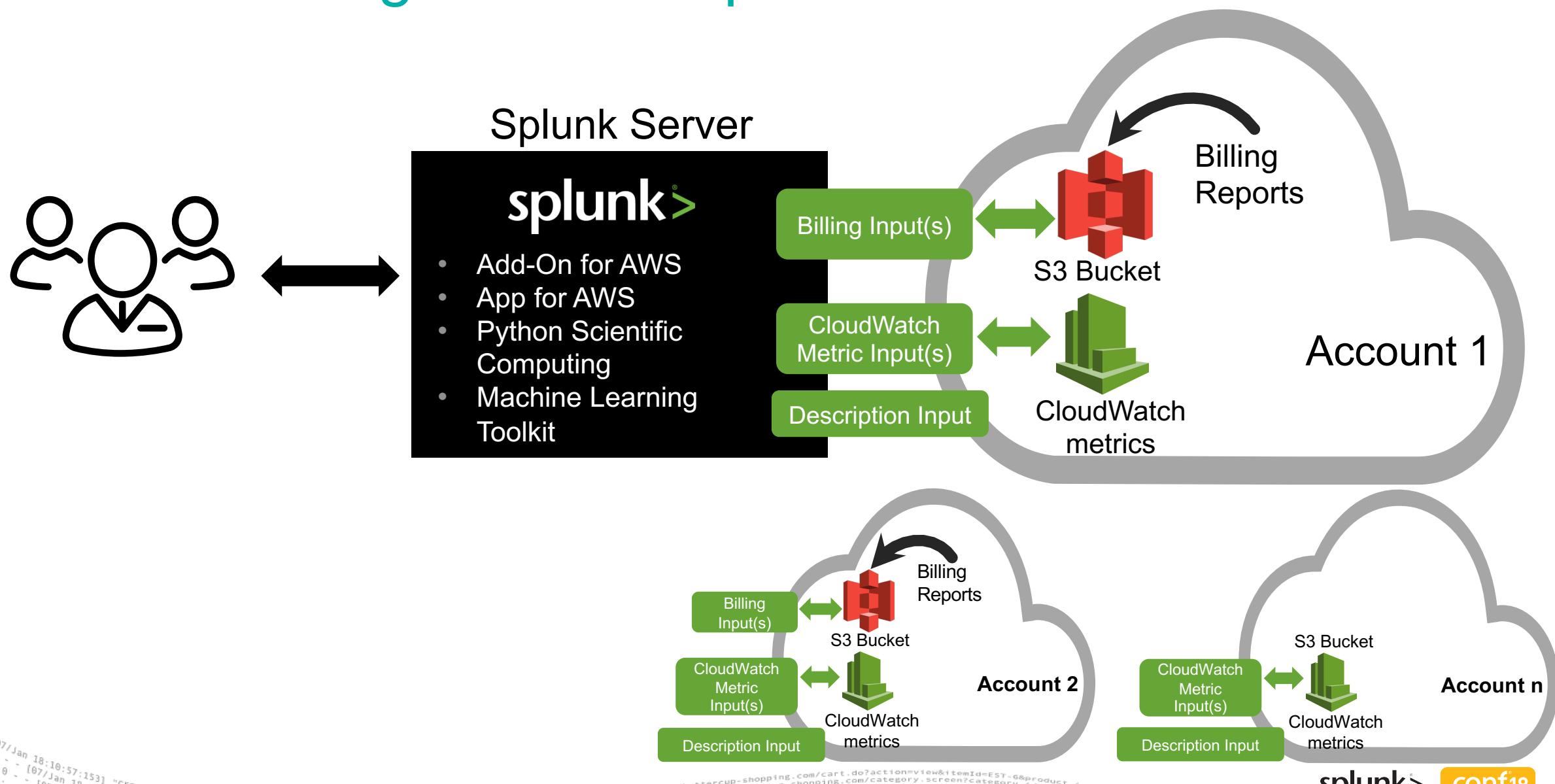
[Save to List](#)

Typical Total Price  
**\$2.136/hr**

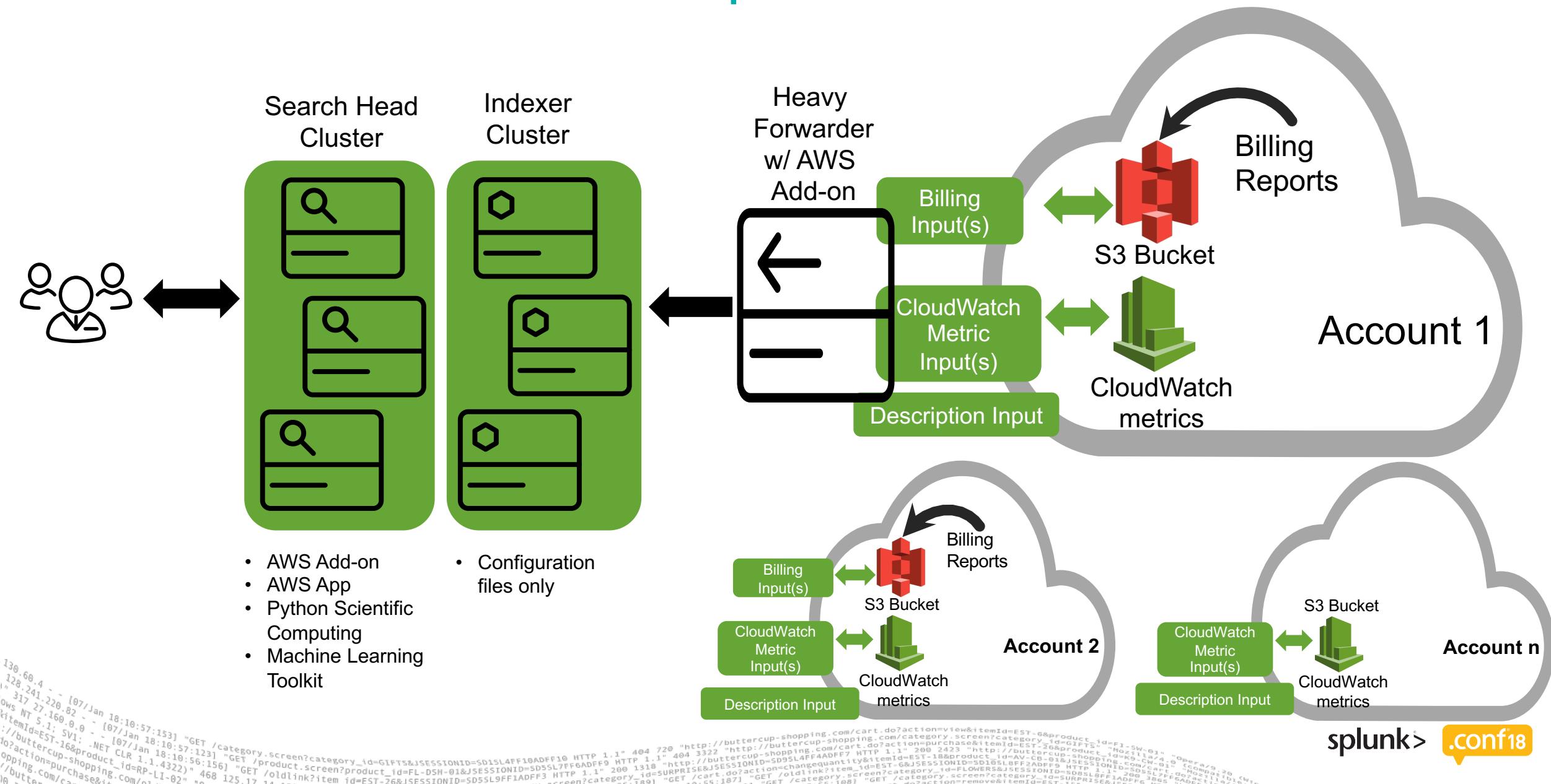
Total pricing per instance for services hosted on t2.xlarge in US East (N. Virginia). [View Details](#)

BYOL option available with  
10, 15, or 20 GB/day

# Single Server Splunk Architecture



# Distributed Splunk Architecture



# Architecture & Sizing Considerations

## Billing

	AWS Considerations	Splunk Consideration
	Billing reports themselves do not incur charges, but standard S3 charges apply.	If relevant, leverage AWS Organizations to Consolidate billing across multiple AWS accounts
		Roughly 20 -100 GB/day without Cost & Usage Report

## CloudWatch

	<ul style="list-style-type: none"> <li>1,000,000 free Cloudwatch API requests/month (translates to anywhere between 2-4 million metrics with 30 minute polling of 5-minute granular data)</li> <li>Consider requesting API input increase if this isn't enough</li> </ul>	<ul style="list-style-type: none"> <li>Create different inputs to match Cloudwatch metric polling frequency (i.e. 1 input for metrics published every 5 minutes, another for billing charge estimate, which is sampled over 4 hours)</li> <li>Updated performance metrics for Add-on 4.6+</li> <li>Pre 4.6: Approx. max of 10,000 metrics / heavy forwarder (approx. 240 metrics/second).</li> <li>Additional heavy forwarders to scale</li> </ul>
--	---	--

[http://docs.splunk.com/Documentation/AddOns/released/AWS/S3PerformanceReference#Measured\\_performance\\_data](http://docs.splunk.com/Documentation/AddOns/released/AWS/S3PerformanceReference#Measured_performance_data)

# Installation Checklist

splunk> .conf18

# Preliminary Setup Summary

For deploying a Splunk AMI acting as a heavy forwarder

## AWS:

- ▶ Create security policy with all necessary permissions, associate with an ec2 service role
- ▶ Associate with Splunk Heavy Forwarder AMI (referenced below)
- ▶ Create security policy with assumeRole permissions for each account (that has CloudWatch metrics of interest and/or Billing reports)

## Splunk:

- ▶ Deploy Splunk AMI in customer's 'central' AWS account as a Splunk Heavy Forwarder (or all-in-one Splunk Instance)

# What is installed & configured where?

## Heavy Forwarder

- ▶ Configure data forwarding to Splunk Indexers (not required for all-in-one AMI)
  - Existing Splunk Cloud instance
  - Existing customer managed on-prem Splunk instance (with Direct Connect or VPN)
  - Existing customer managed Splunk instance in customer AWS account
- ▶ Define new Splunk index(es) for data to reside (for dropdown selection in UI only)
- ▶ Install **Splunk Add-on for AWS**
- ▶ Within AWS Add-on (after Indexers & Search Heads are configured)
  - setup assumeRole or keys for every account
  - add Description input for every account (some AWS app dropdowns dependent on this input)
  - Add CloudWatch metric input for every account; enable metrics for all utilized services
  - Add Billing Input(s) for master account and any other billed account

# What is installed & configured where?

## Indexers

- ▶ Define new user defined Splunk index(es) for data to reside
- ▶ Distribute indexes.conf from **Splunk Add-on for AWS** to the indexers; this includes all summary indexes; do NOT deploy the entire add-on to the indexers
- ▶ (optional, not required for CloudWatch Metrics or Billing Reports)  
Install **Splunk Add-on for AWS**
  - Might only be necessary if HECs are enabled on indexers for other use cases
  - Consultant with Splunk PS or account team on creating a lighter version with required props/transforms/indexes/etc.

# What is installed & configured where?

## Search Head(s)

- ▶ Install **BUT DO NOT CONFIGURE** Splunk Add-on for AWS (*hide the add-on as a best practice*)
- ▶ Install **Splunk App for AWS**
- ▶ Install **Python Scientific Computing Add-on**
- ▶ Install **Machine Learning Toolkit**
- ▶ Update all macros with the names of indexes used (i.e. you create an index named ‘aws\_data’ and specify all inputs to write to this index; update the **aws-billing-index** macro to *index=aws\_data*)
- ▶ Enable tag filtering for billing reports
- ▶ Setup Search Heads to forward data to indexing tier

# Install & Configuration References

- ▶ Conf2018 session on GDI (Getting Data In): IT1452

- ▶ Configure AWS Services Documentation

<https://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWS>

- ▶ Configure AWS Permissions Documentation

<https://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSPermissions>

- ▶ AWS Add-on Installation Documentation

<https://docs.splunk.com/Documentation/AddOns/released/AWS/Distributeddeployment>

- ▶ AWS App Installation Documentation

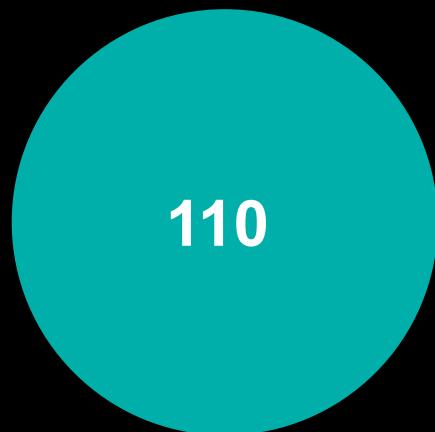
<https://docs.splunk.com/Documentation/AWS/latest/Installation/Installon-prem>

# Takeaways



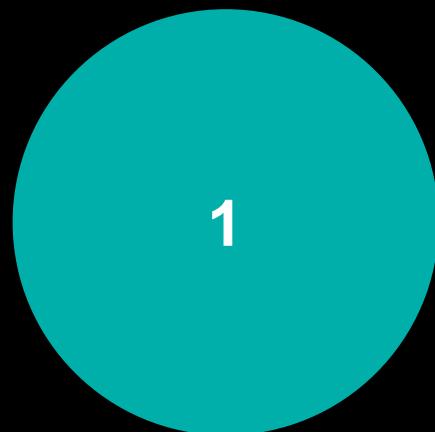
unlimited

Number of accounts you  
can manage with Splunk  
App & Add-on for AWS



110

Number of out of box  
dashboards & reports



1

Location to report &  
correlate data

# Customer Success Stories

## FINRA Uses Splunk Cloud for Transparency and End-To-End Visibility in AWS



“Splunk Cloud gives you applications that let you get huge amounts of value from your data.”

– *Sr. Director, Information Security*

- ▶ Comprehensive security visibility leveraging AWS CloudTrail
- ▶ Real-time AWS cost management reducing spend on select AWS workloads by over 50%
- ▶ Correlating data across hybrid environment spanning AWS and on-premises

# Real-Time Car Auctions Delivered With Intelligence



“With Splunk ITSI, we have proactive infrastructure monitoring to ensure a consistent level of customer service for interested buyers to bid on cars.”

– *VP Technology Application Development & Operations, Cox Automotive*

- ▶ Reduced time-to-investigate and resolution with real-time insights
- ▶ Reduced incidents across global auctions by 90%
- ▶ Improved end-user experience and service reliability
- ▶ Scaling the implementation with Splunk Cloud & visualizing AWS Cloudtrail and Amazon VPC Flow Logs with App for AWS



Cox  
AUTOMOTIVE™

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

