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> .conf18

#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 Challenges

The Reality

…is **AWS**ome.

- 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

66%

Customers acknowledging ‘significant’ problems managing AWS spend

25%

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/

splunk> .conf18

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

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

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

splunk> .conf18

Splunk App for AWS – Capacity & Cost Mgmt Dashboards

Overview | Topology | Timeline | Usage | Security | Insights | Billing | Search

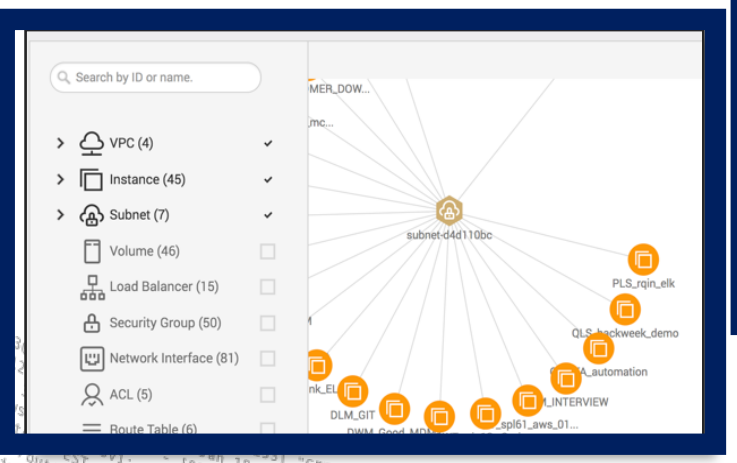
- Overview
- Usage Overview
- Security Overview
- Insights Overview
- Anomaly Detection Overview

- EC2 Instances
- Individual EC2 Instances
- EBS Volumes
- Individual EBS Volumes
- ELB Instances
- Individual ELB Instances
- Relational Database Service
- Lambda
- API Gateway
- Capacity Planner
- Reserved Instance Planner
- Reserved Instance Inventory

- Network ACLs
- Security Groups
- IAM Activity
- Key Pairs Activity
- S3 - Data Event
- VPC Activity
- Resource Activity
- User Activity
- CloudFront - Traffic Analy
- ELB - Traffic Analysis
- S3 - Traffic Analysis
- VPC Flow Logs - Traffic Analysis
- VPC Flow Logs - Security Analysis

- Config Rules
- Amazon Inspector
- EC2 Insights
- ELB Insights
- EBS Insights
- Elastic IP Insights
- Security Group Insights
- IAM Insights

- Budget Planner
- Current Month Estimated Billing
- Historical Monthly Bills
- Historical Detailed Bills



splunk> .conf18

Fun fact

#1

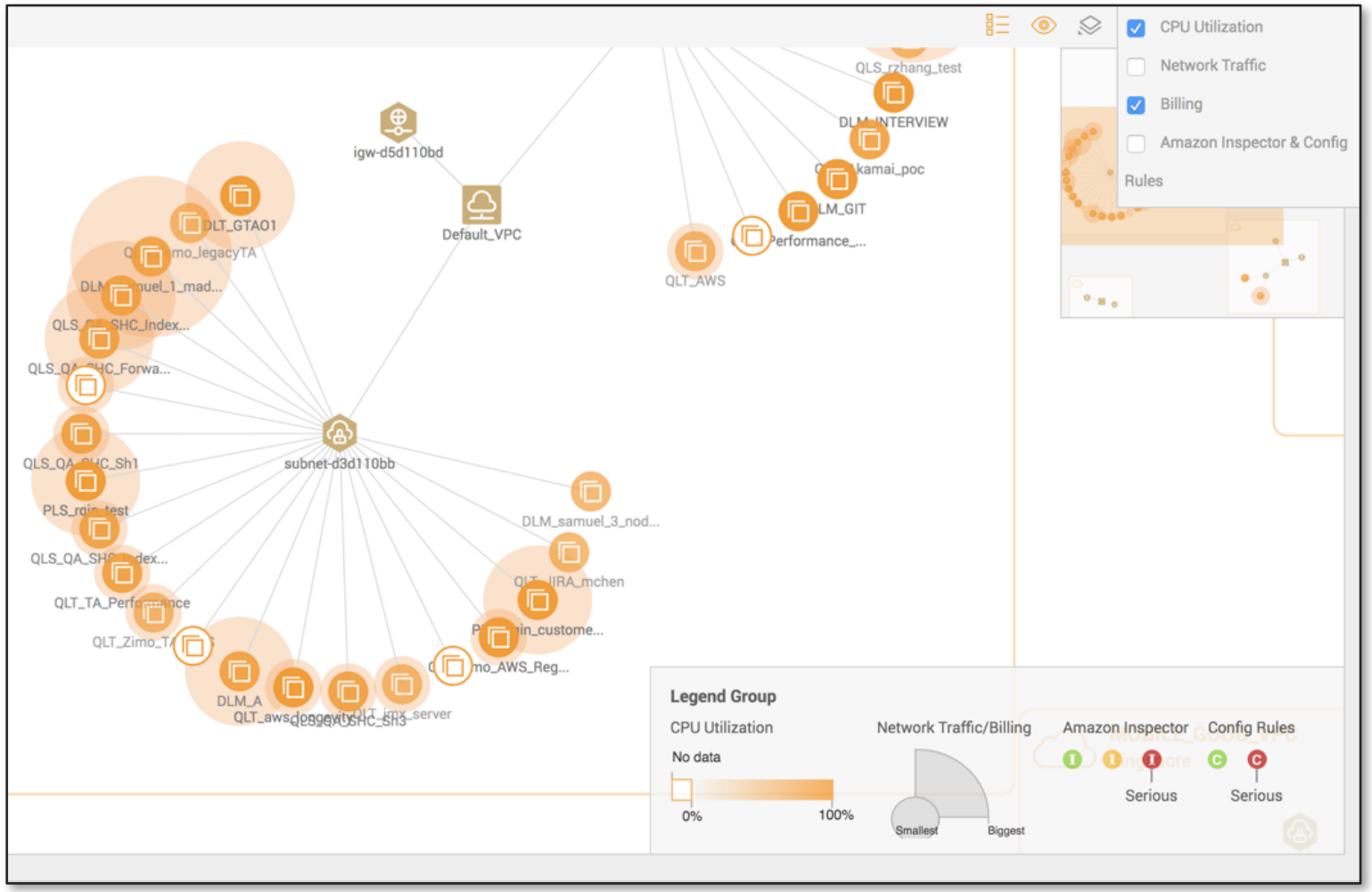
AWS Billing Reports
are the
most accessed
in the
Splunk App for AWS
Amongst Splunk Cloud customers

Splunk App for AWS – Topology View

Topology can be overlaid with:

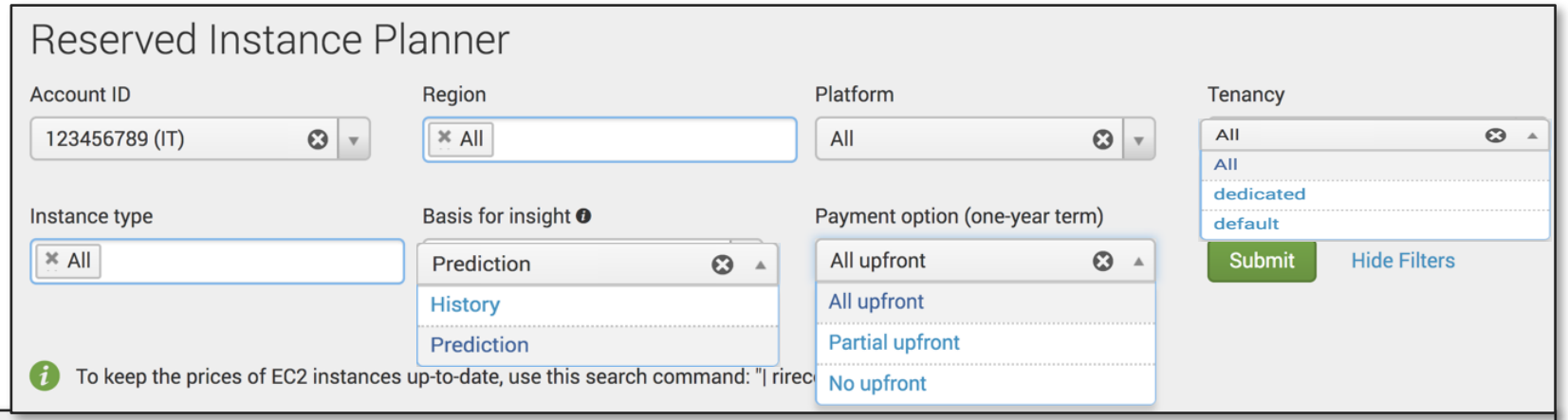
- Resource Cost indicator
- Resource usage indicator

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?



To keep the prices of EC2 instances up-to-date, use this search command: "| rirecommendation 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

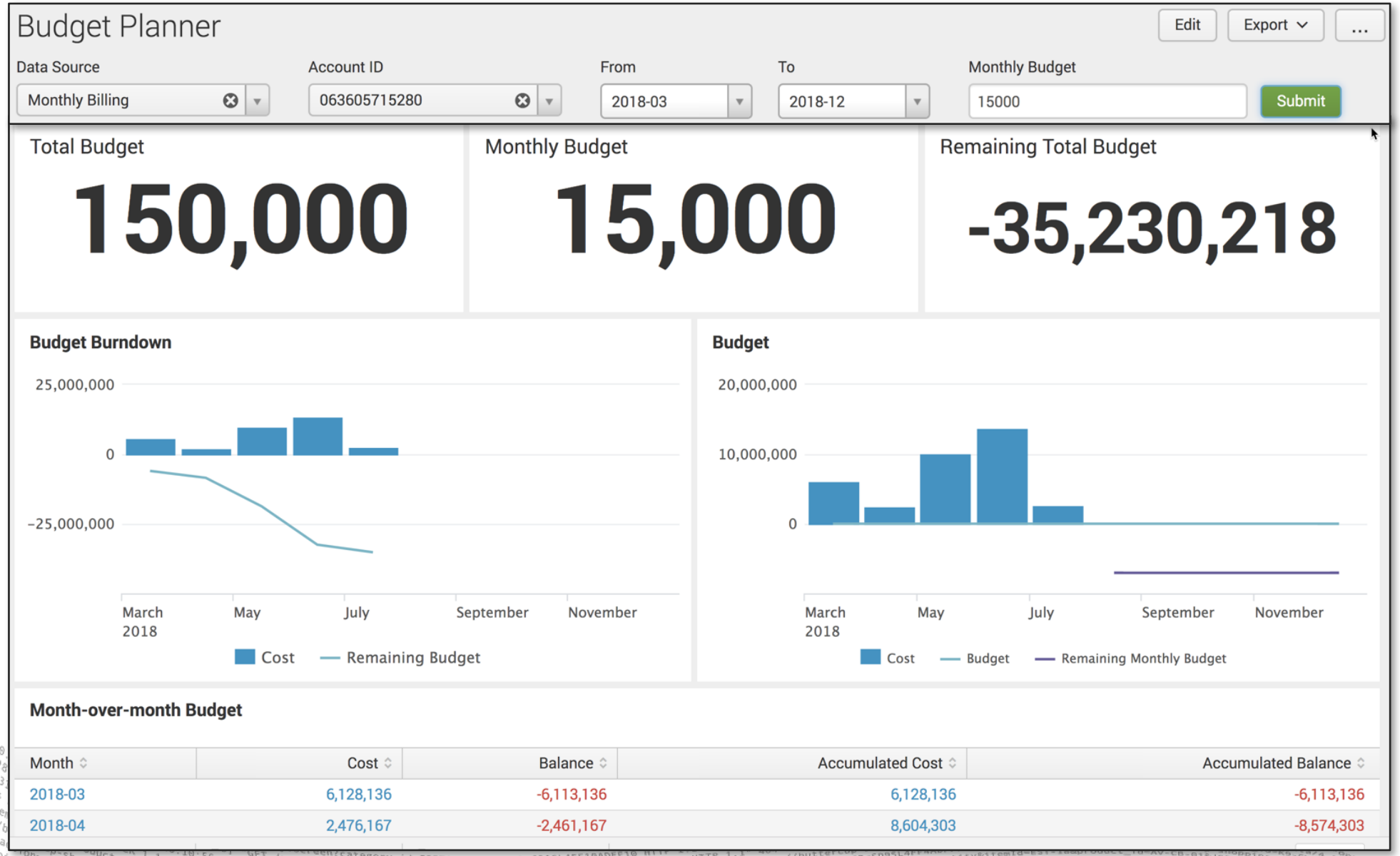
Hide Messages

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	Details
>	123456789	China (Beijing)	Linux/UNIX	default	m4	0 (unit)	148 (unit)	¥261,204	Details
v	123456789	Asia Pacific (Singapore)	Linux/UNIX	default	d2	0 (unit)	240 (unit)	$107,808	Details
>	123456789	EU (Frankfurt)	Linux/UNIX	default	d2	0 (unit)	240 (unit)	$95,275	Details
>	123456789	Asia Pacific (Sydney)	Linux/UNIX	default	d2	0 (unit)	120 (unit)	$53,944	Details

Existing RIs:
You already had 0 reserved instance in this category, converting to unit : 0.
Optimal RIs:
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:

- 240 = 240 x 1 (small)

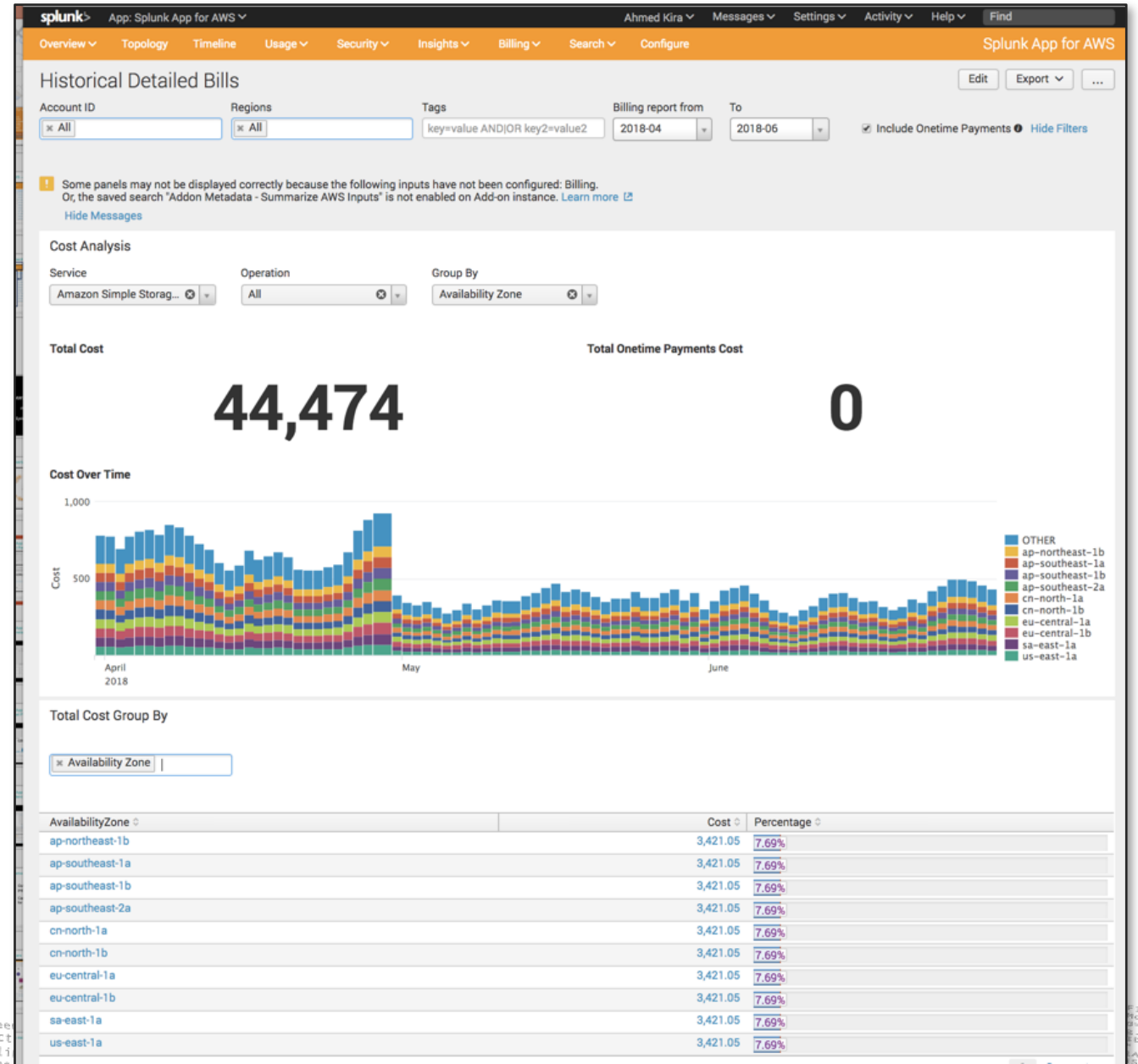
Splunk App for AWS – Budget Planner



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

splunk> .conf18

Splunk App for AWS – Detailed Billing



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

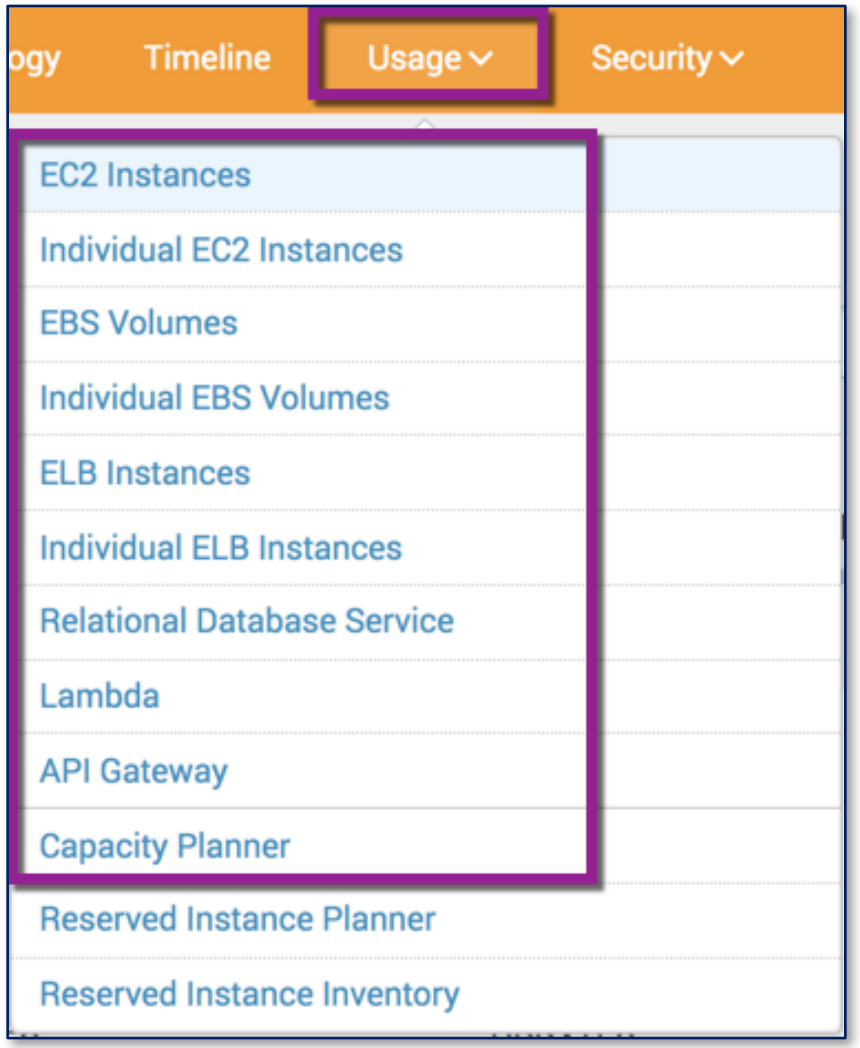
splunk> .conf18

Capacity Planning Dashboards

Section subtitle goes here

splunk> .conf18

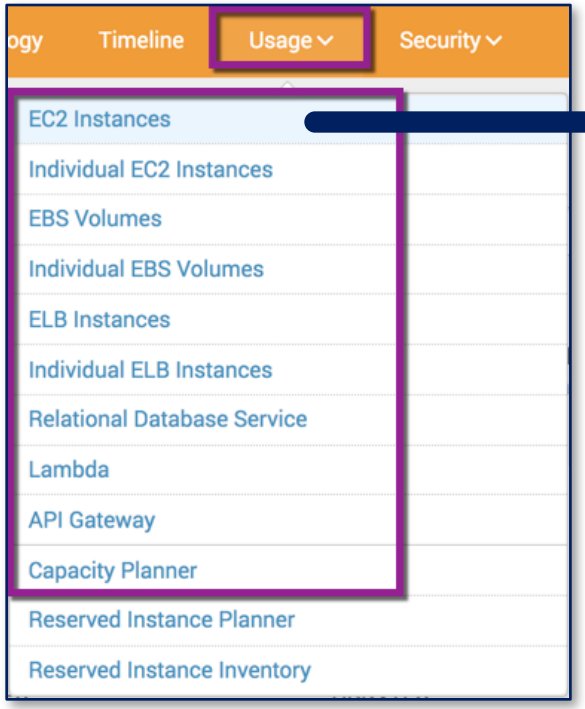
Capacity Management Relevant Views

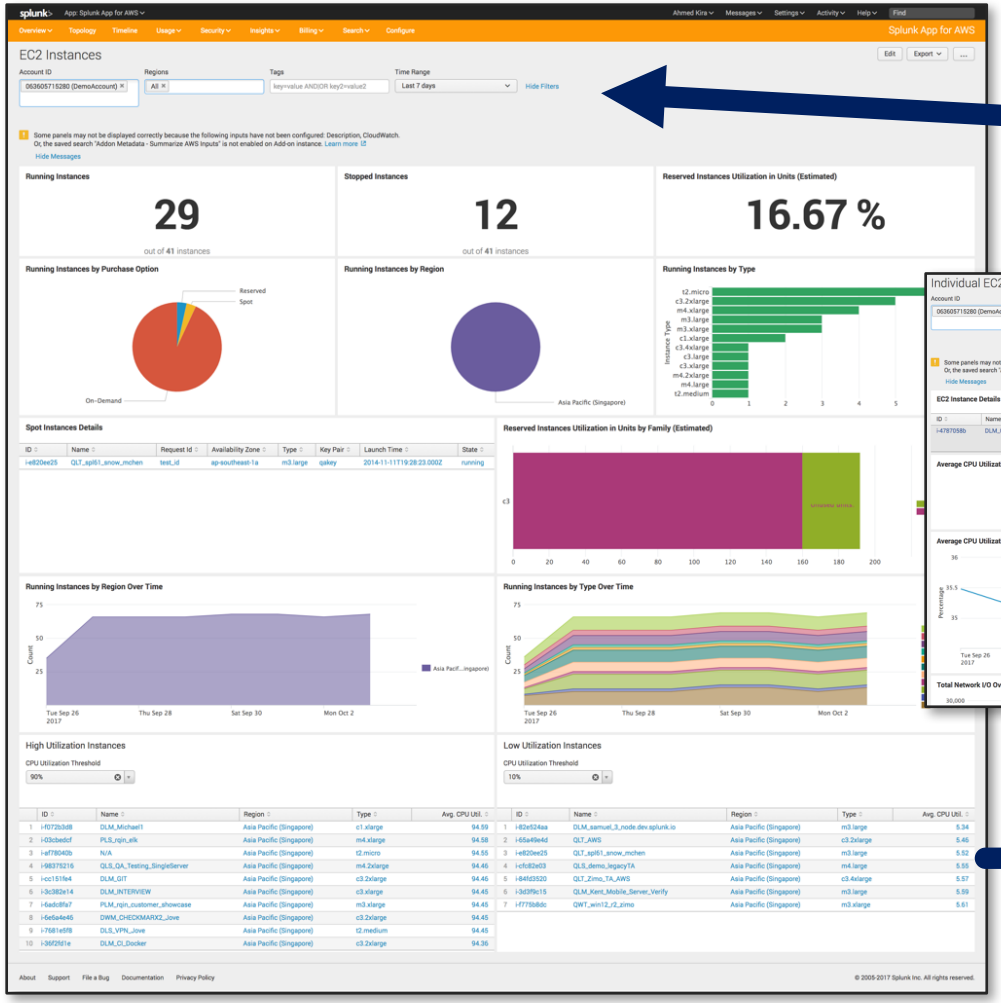


Out of box dashboards for popular AWS Services

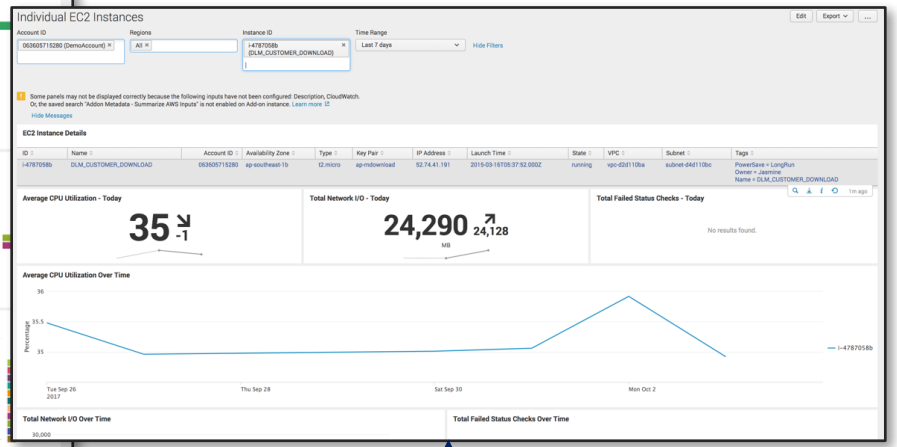
Can be leveraged as templates for custom dashboards

What EC2 instances are over or under utilized?



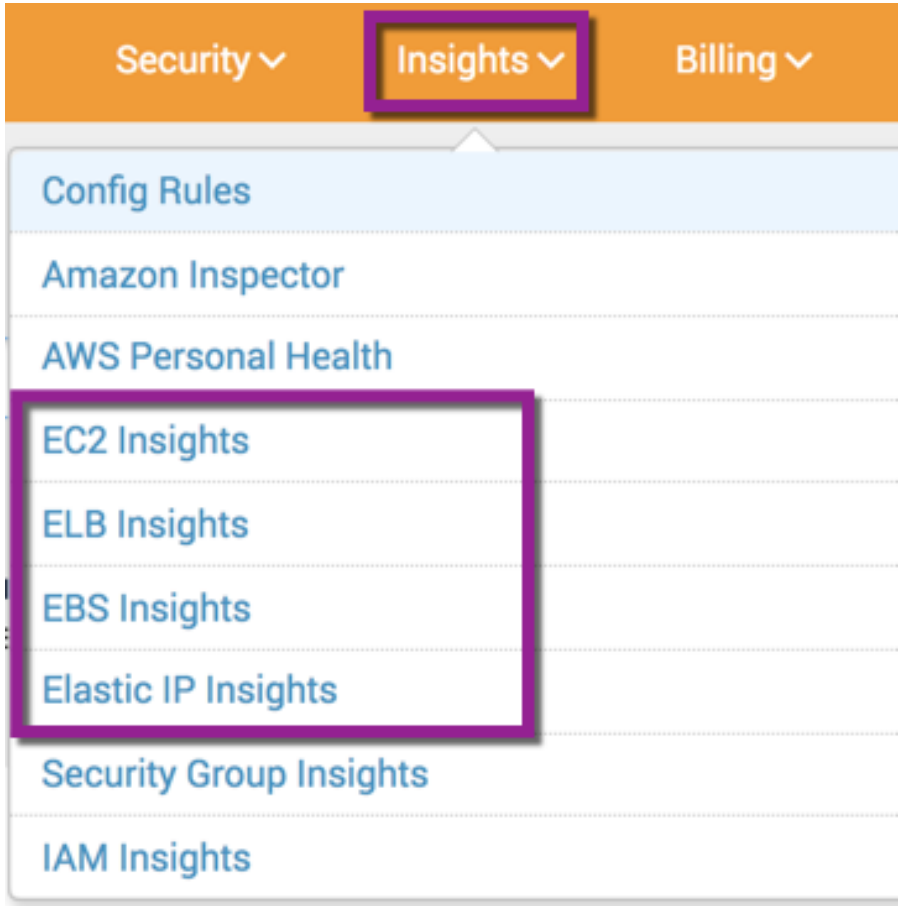


Filter by Account, Region, Tag



Drill into under-utilized or over-utilized instance details

Insights dashboards



What EBS volumes are unused?

What ec2 instances need to be upgraded?

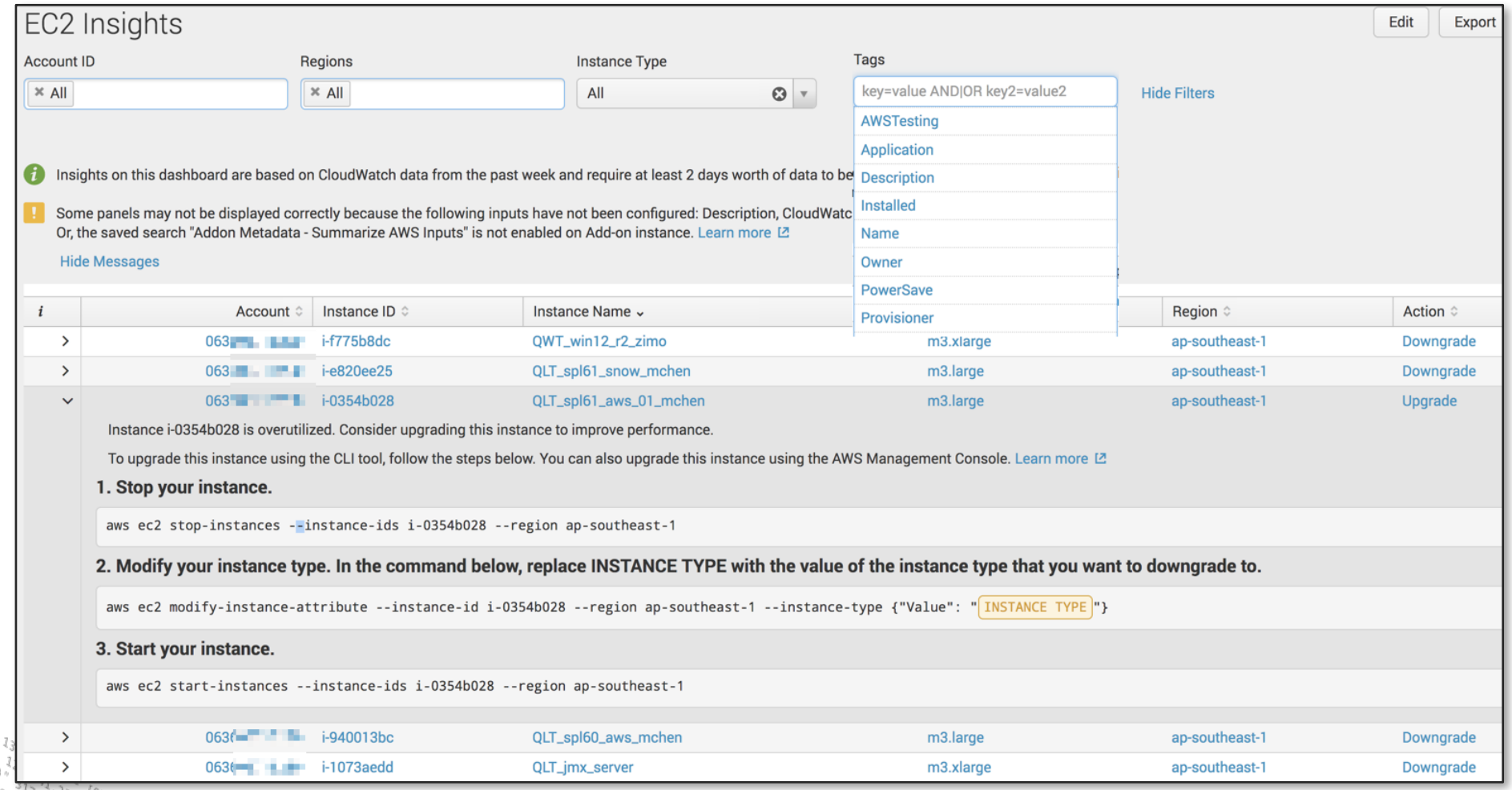
What ec2 instances need to be downgraded?

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



Features

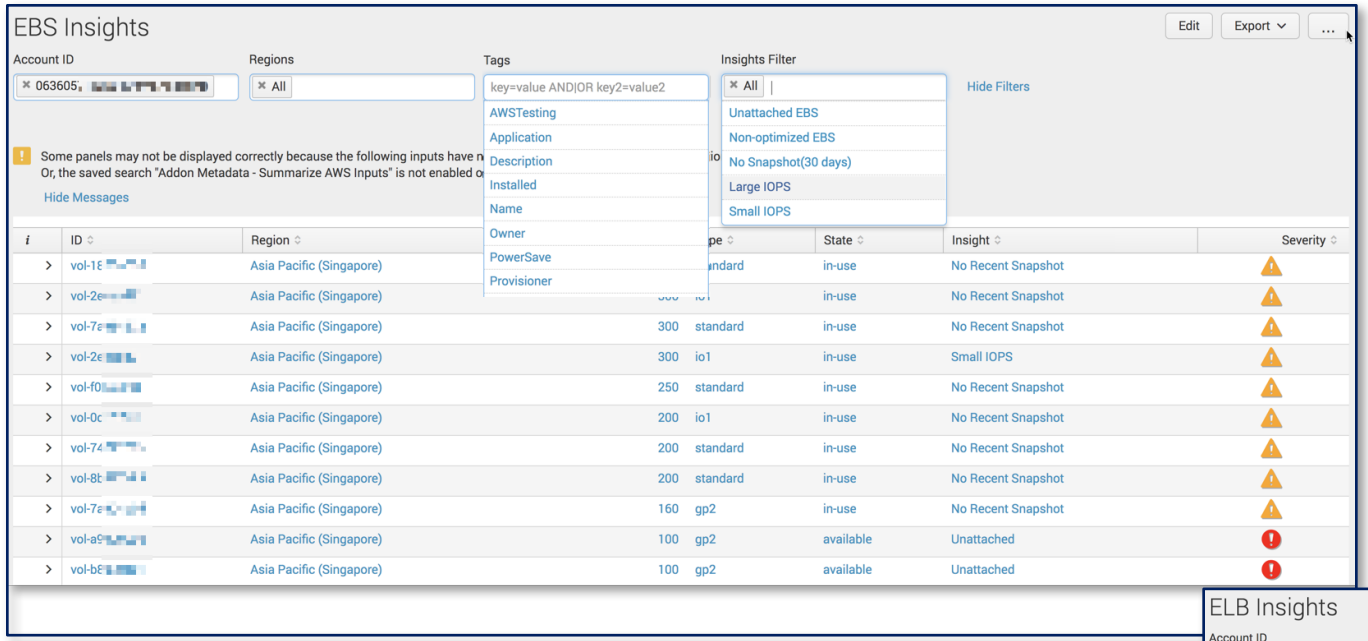
- Determine which instances need to be right-sized
- Copy/Paste commands to AWS CLI
- Filter by tag, region, account

Value Realized

- Maintain costs without sacrificing performance

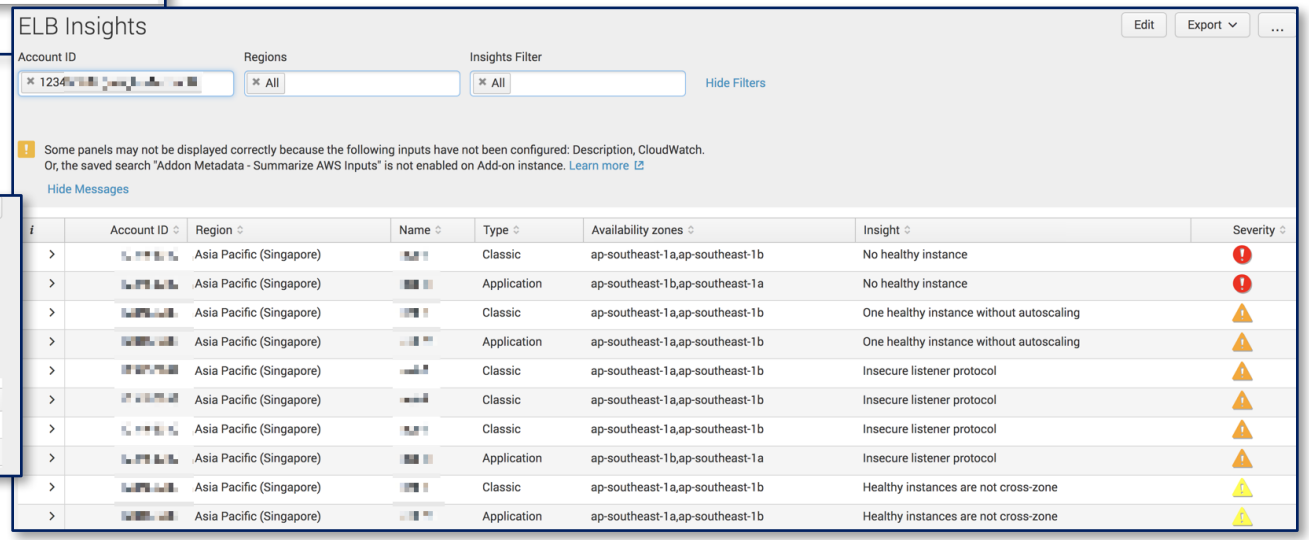
splunk> .conf18

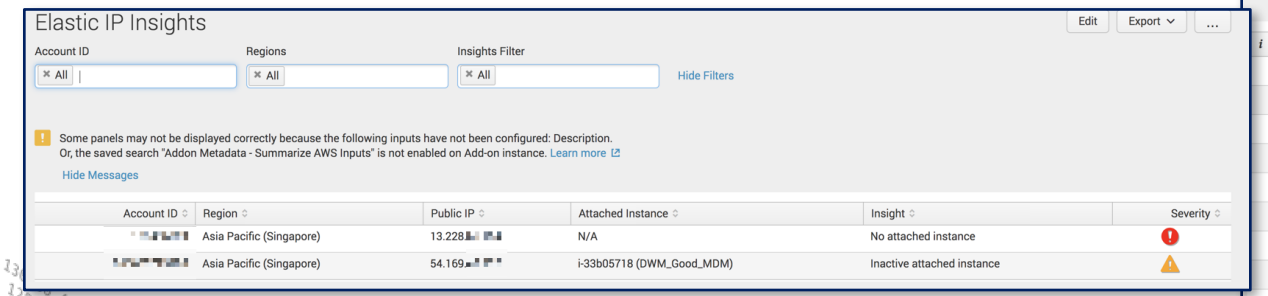
More Insights for popular AWS services



Eliminate unused services

Add capacity for unhealthy Load Balancer or low IOPS volumes





splunk> .conf18

Takeaways on Why Splunk?

unlimited

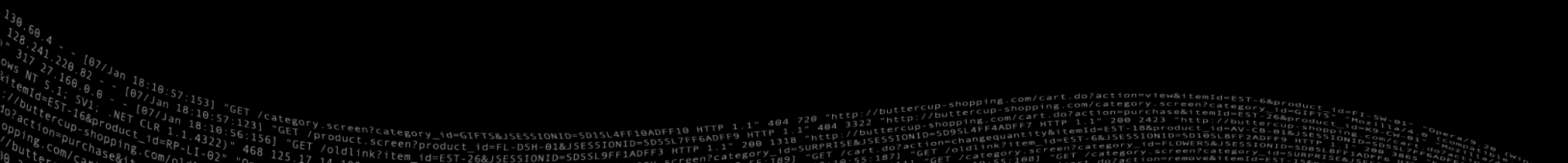
Number of accounts you can manage with Splunk App & Add-on for AWS

110

Number of out of box dashboards & reports

1

Location to report & correlate data



splunk> .conf18

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

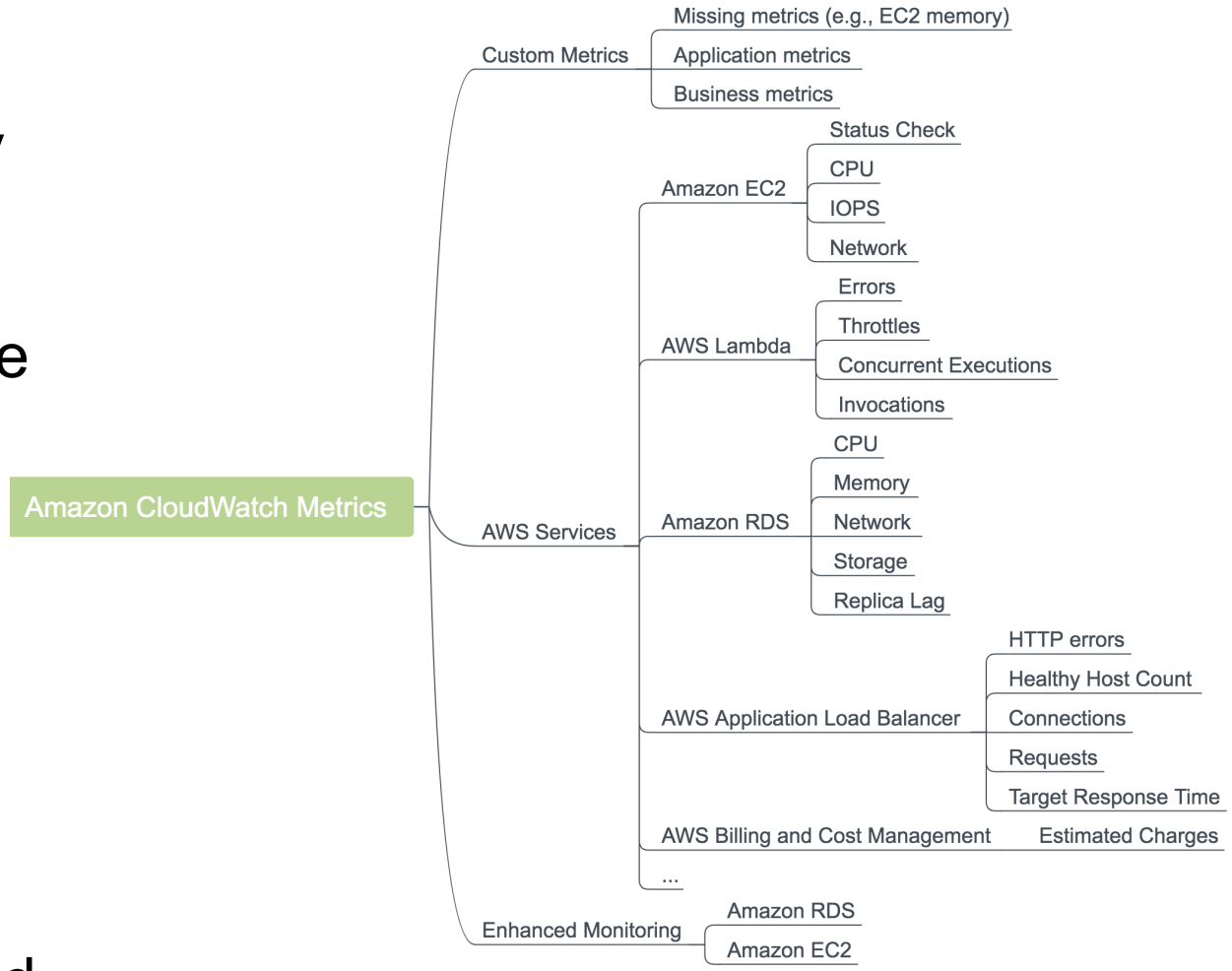
AWS CloudWatch Metrics

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/

splunk> .conf18

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": "*"
    }
  ]
}
```

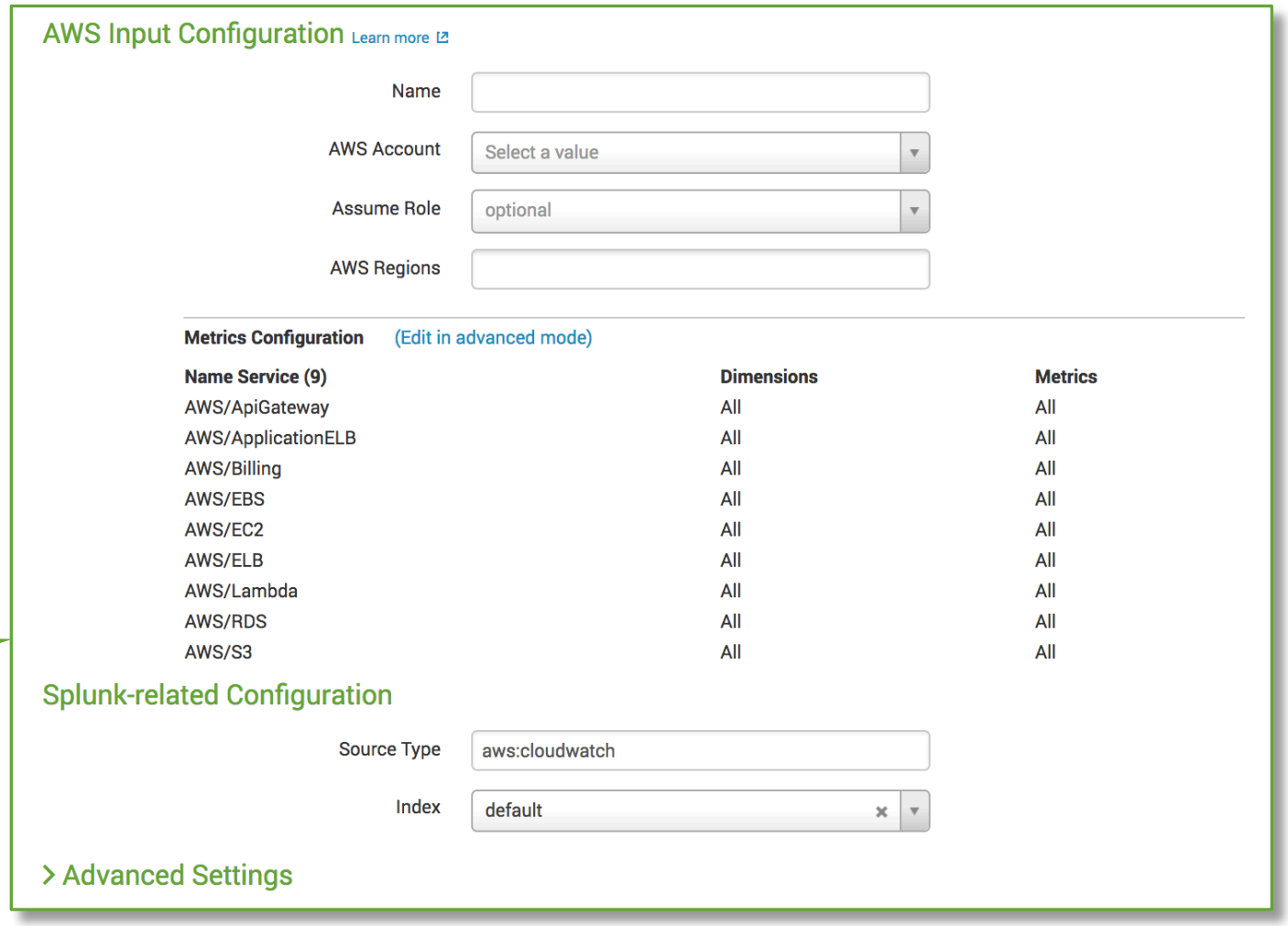
Documentation:
https://docs.splunk.com/Documentation/AddOns/released/AWS/ConfigureAWSpermissions#Configure_CloudWatch_permissions

splunk> .conf18

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

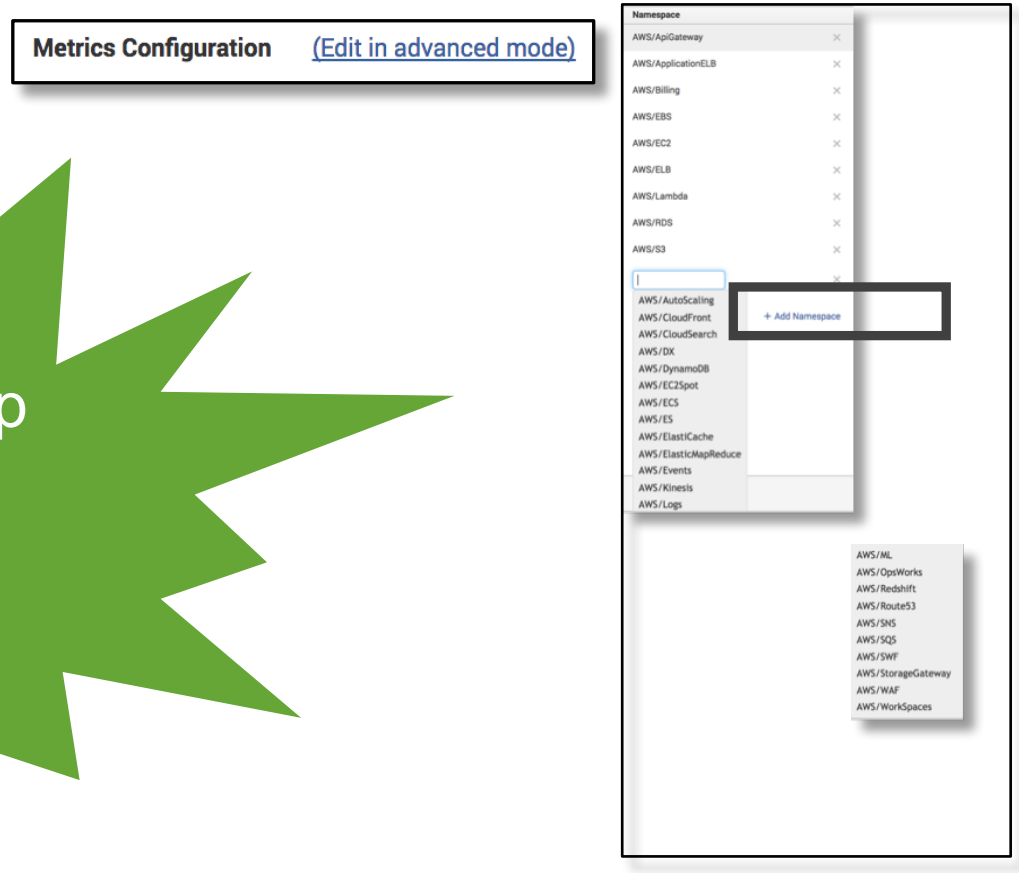
Notice AWS/Billing is enabled by default

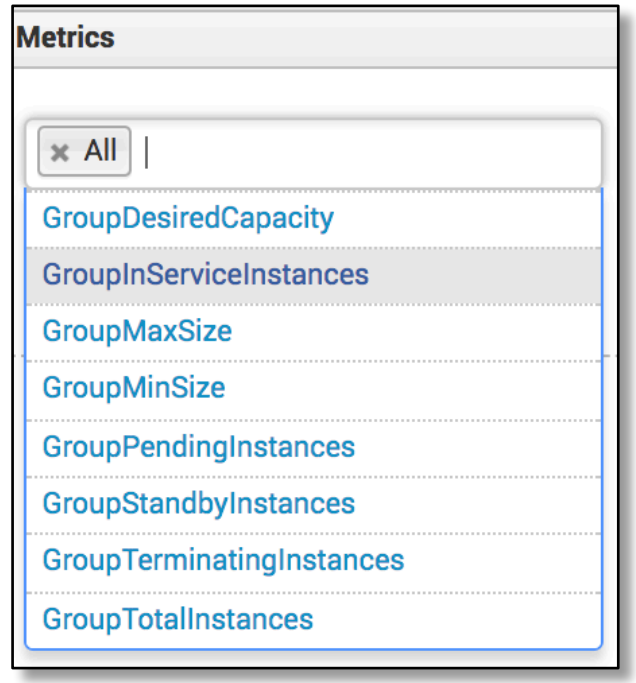


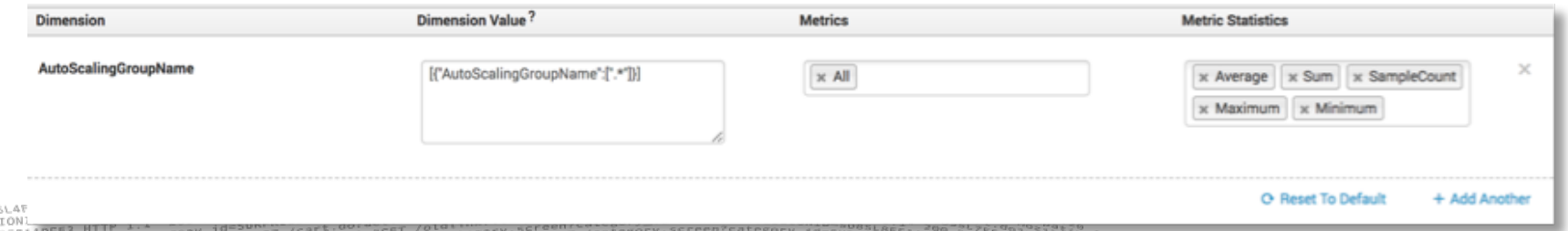
splunk> .conf18

What about CloudWatch metrics from other namespaces?

Simplified setup for enabling additional CloudWatch metrics





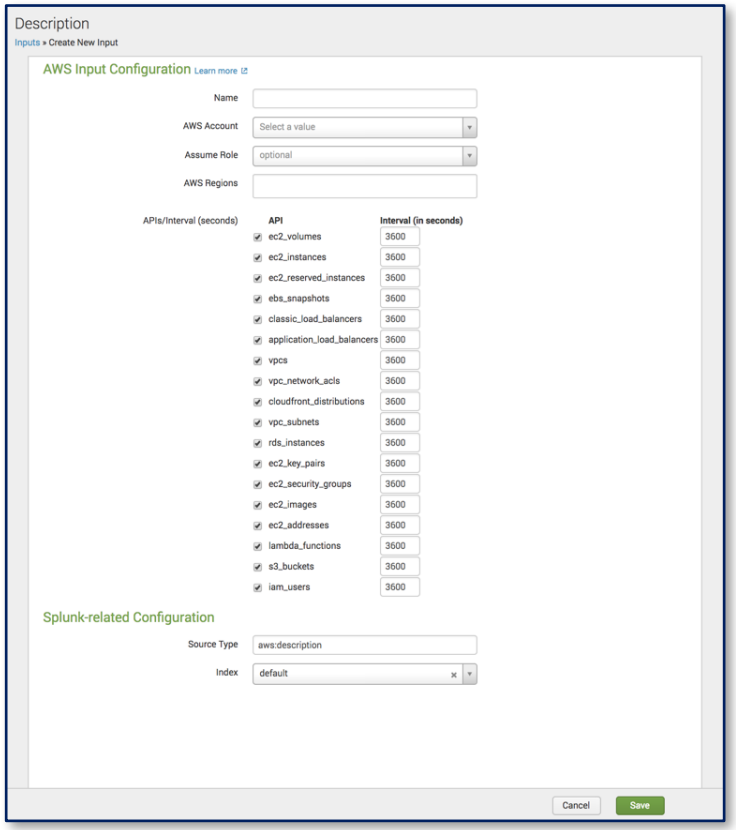


Required Description Input & Permissions

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": [
        "*"
      ]
    }
  ]
}
```



splunk> .conf18

Billing Reports

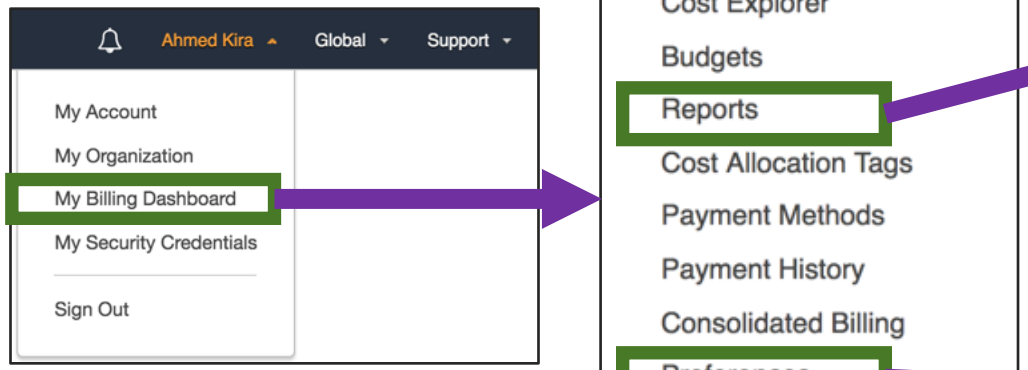
Relevant AWS Billing Data

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	

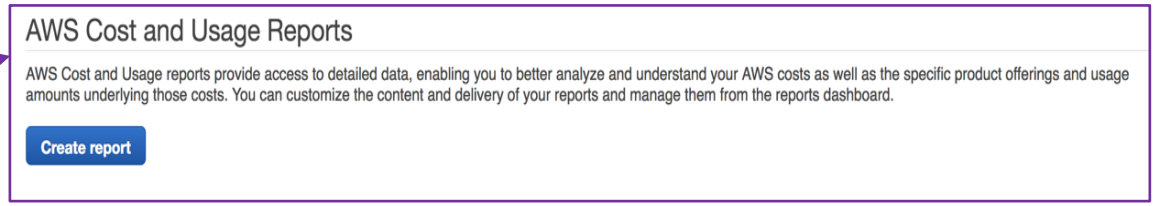
Recommended reports to make available for Splunk

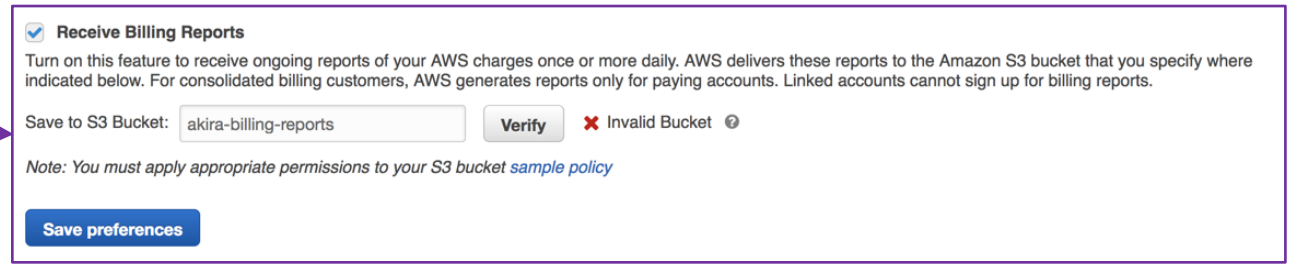
Data Source	Ingest Method	Collection Interval	Sourcetypes / Event Types	Reports / Dashboards
Monthly Report	Billing Input (read through API)	Daily Snapshot (Month to Date Totals)	Sourcetype: aws:billing Eventtype: aws_billing_monthly_report	“Total” or “monthly” reports & dashboards
Monthly Cost Allocation 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





- ‘Traditional’ reports
- CloudWatch Billing metrics

splunk> .conf18

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"
      ]
    }
  ]
}
```

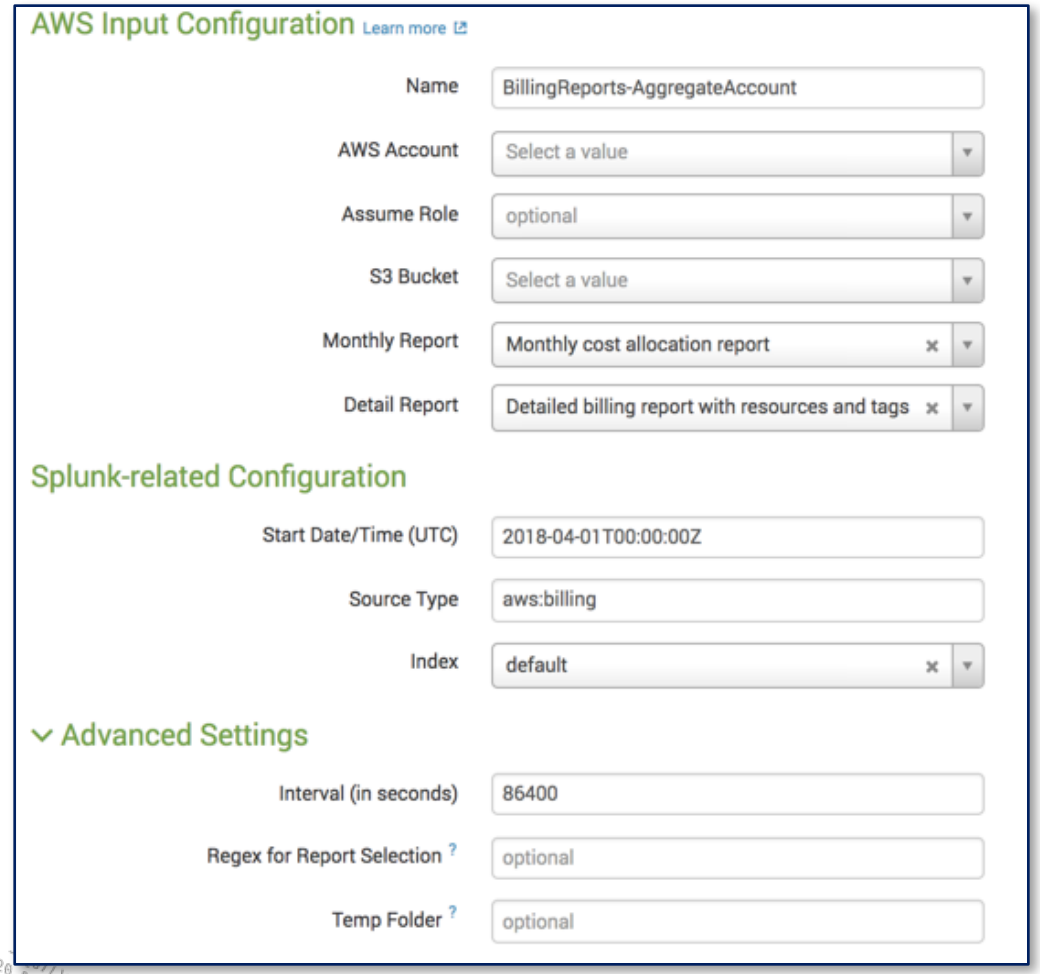
- Within account/role that Splunk Add-on runs as:
  - If policy is defined on master account billing S3 bucket, no additional steps required.
  - assumeRole option if a different role has the required permissions

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

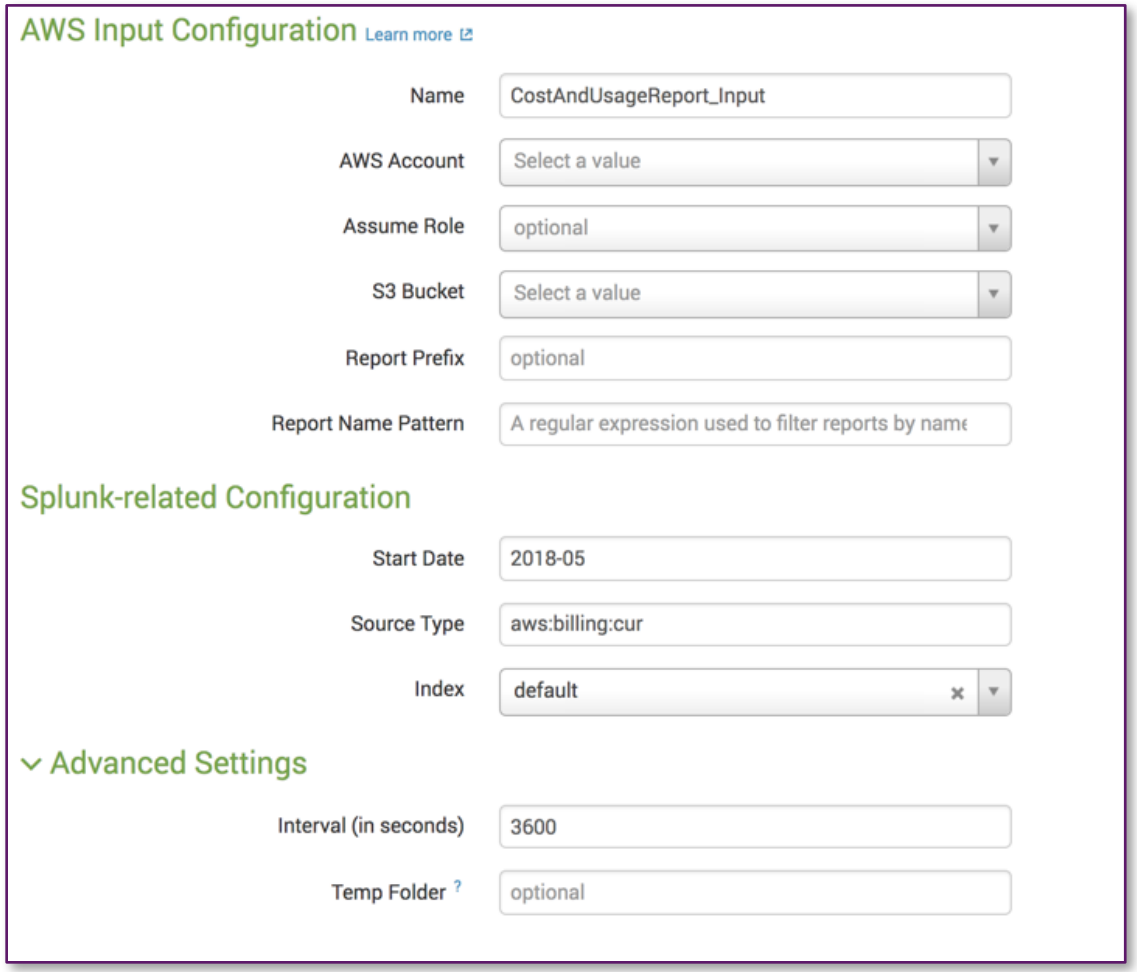
splunk> .conf18

Billing Inputs within Splunk Add-on for AWS

Traditional Billing Input



Cost & Usage Report Input

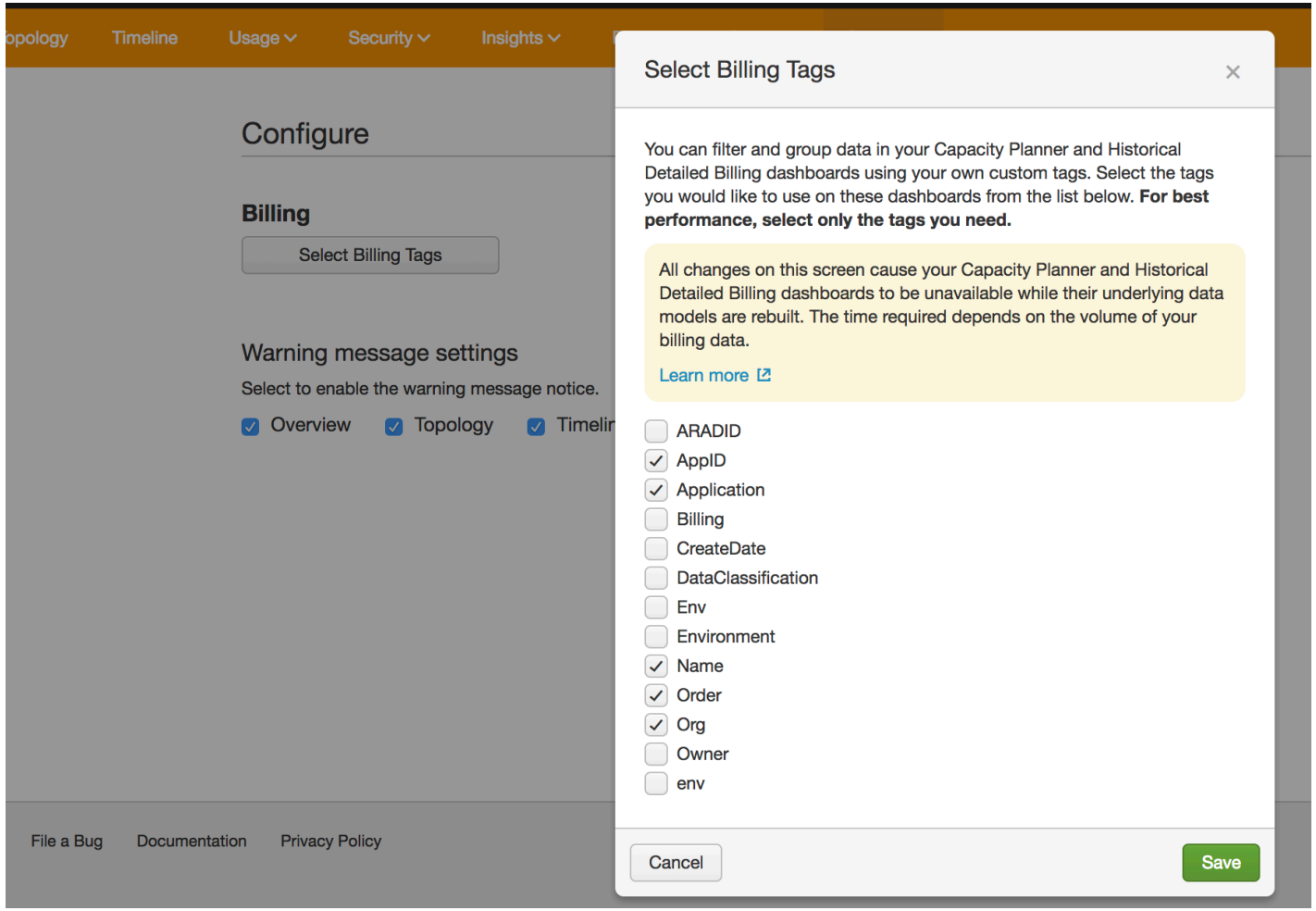


splunk> .conf18

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)



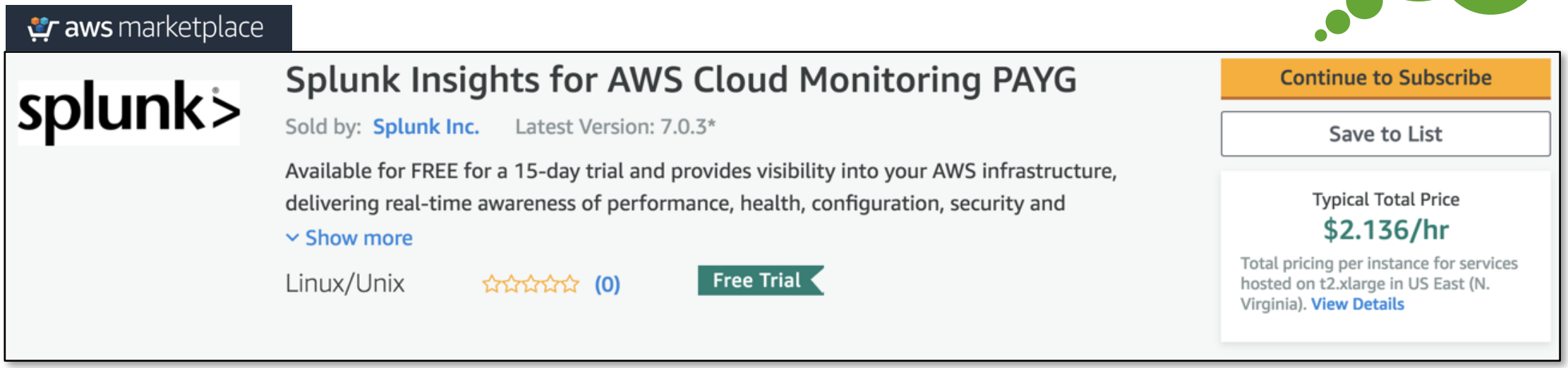
splunk> .conf18

Splunk Setup & Considerations

Want AWS Only Visibility?

Splunk Insights for AWS Cloud Monitoring

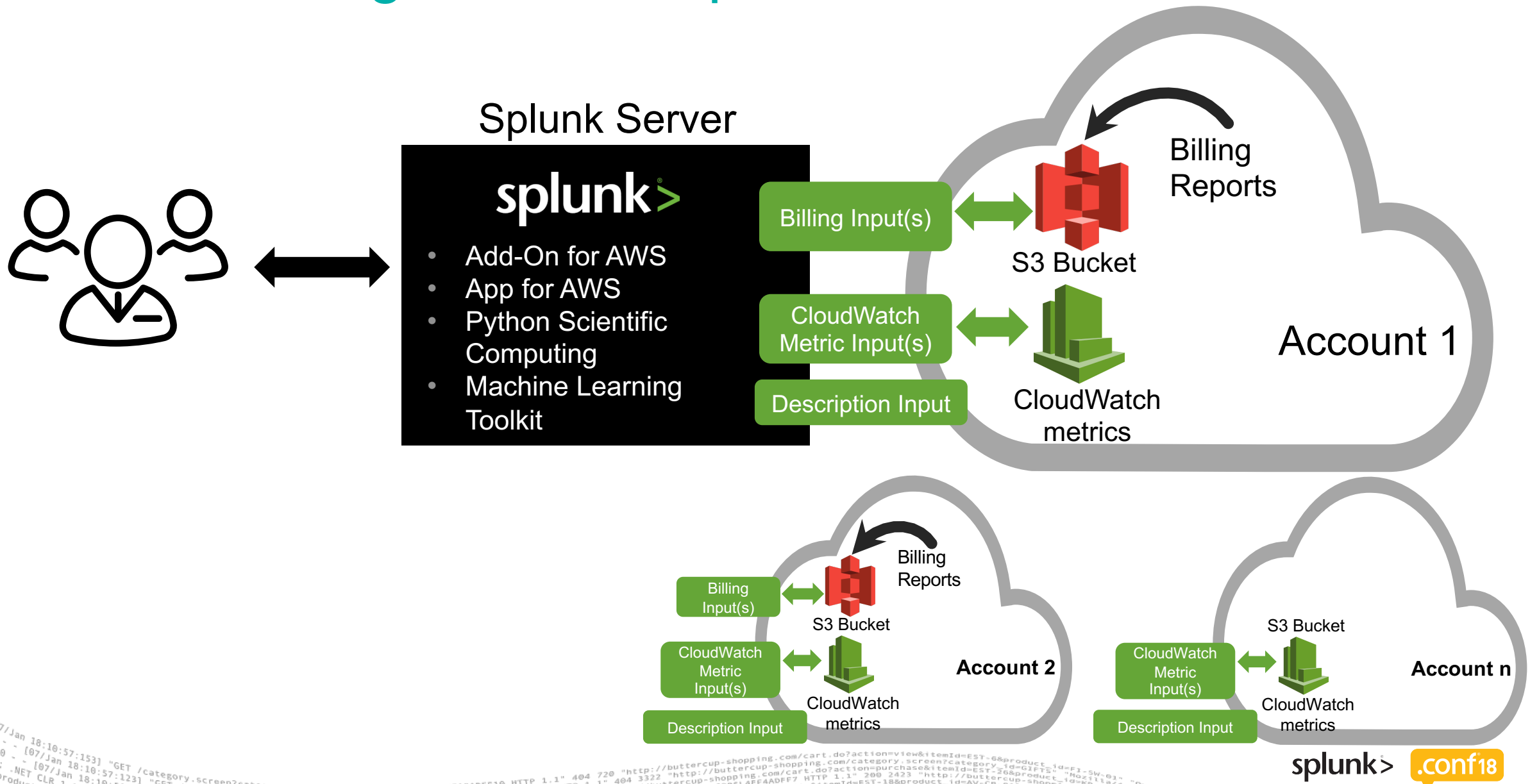
Setup for max 10 GB/day



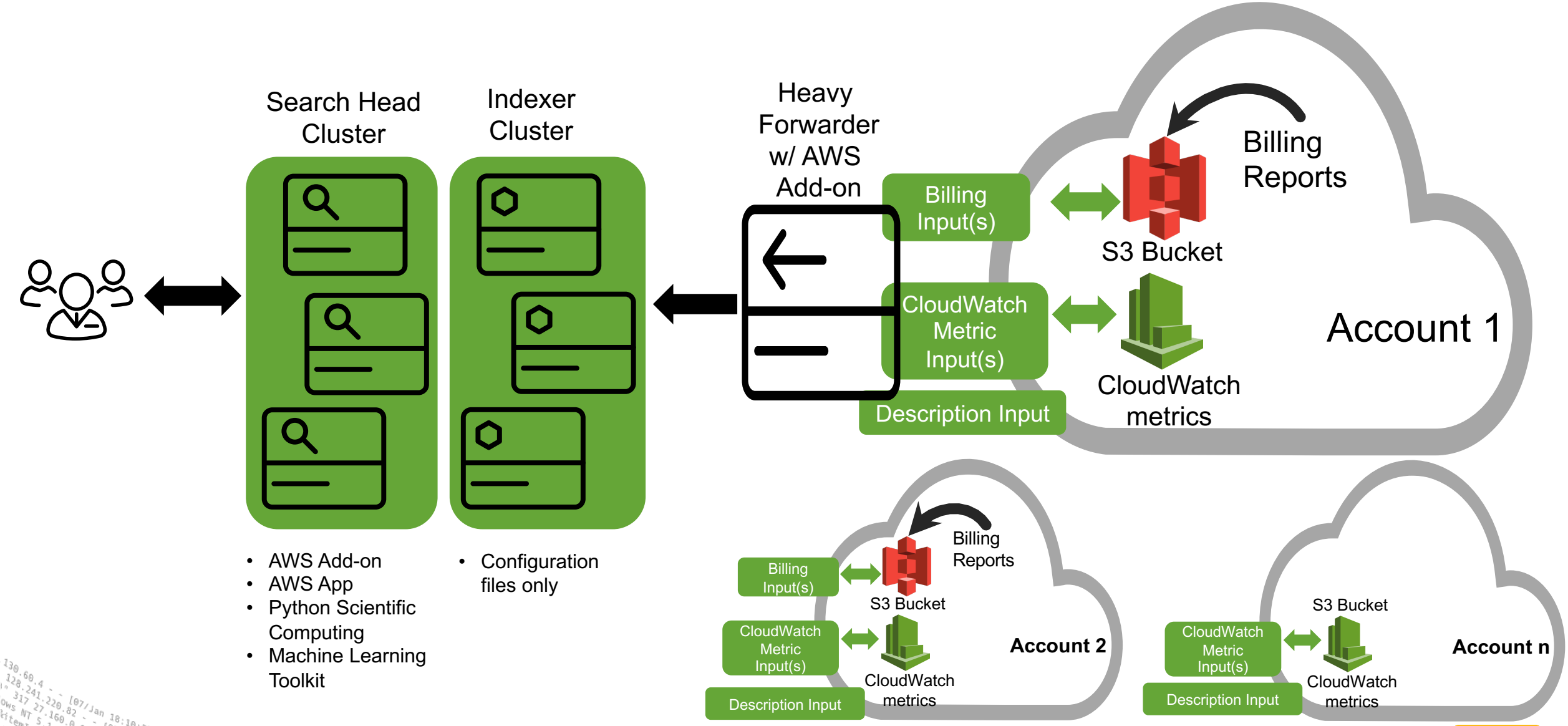
BYOL option available with 10, 15, or 20 GB/day

splunk> .conf18

Single Server Splunk Architecture



Distributed Splunk Architecture



splunk> .conf18

Architecture & Sizing Considerations

	AWS Considerations	Splunk Consideration
Billing	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	• 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) • Consider requesting API input increase if this isn't enough	• 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)
		• Updated performance metrics for Add-on 4.6+ • Pre 4.6: Approx. max of 10,000 metrics / heavy forwarder (approx. 240 metrics/second). • Additional heavy forwarders to scale
		• Don't forget to account for other inputs

http://docs.splunk.com/Documentation/AddOns/released/AWS/S3PerformanceReference#Measured_performance_data

Installation Checklist

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)

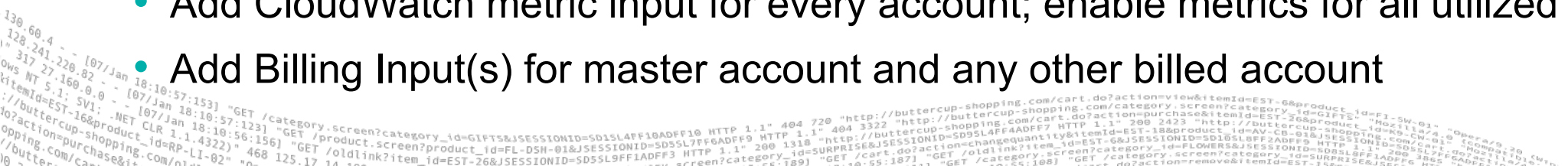
Splunk:

- 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

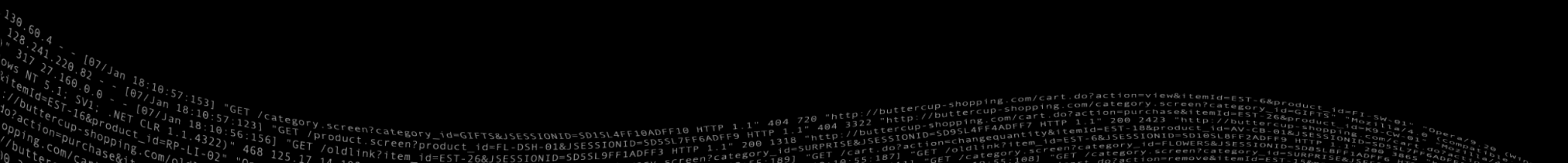
Number of accounts you can manage with Splunk App & Add-on for AWS

110

Number of out of box dashboards & reports

1

Location to report & correlate data



Customer Success Stories

splunk> .conf18

FINANCIAL SERVICES – CLOUD SOLUTIONS, SECURITY

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

ONLINE SERVICES – CLOUD SOLUTIONS, IT OPERATIONS

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

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