Manage AWS Services

Cost, Security, Best Practice and Troubleshooting

Elias Haddad  |  Principal Product Manager
Peter Chen  |  Principal Software Engineer

September 2017  |  Washington, DC
Agenda

- Challenges in Managing Enterprise Level AWS Services
- Get Data In – AWS Add-on
- Data Analysis and Visualization – AWS App
- Case Study
- Q & A
Challenges in Managing Enterprise Level AWS Services

Cost Optimization

- Multi accounts
- Budget planning
- RI planning
- Cost forecasting
- Anomaly detection
- Smart alerting
Challenges in Managing Enterprise Level AWS Services

Cost Optimization

Security Strategy

- Access monitoring
- API call monitoring
- User management
- Anomaly detection
- Smart alerting
Challenges in Managing Enterprise Level AWS Services

Cost Optimization

Security Strategy

Best Practice

- Config Rule
- Inspector
- EC2
- ELB
- EBS
- EIP
- SG
- IAM
Challenges in Managing Enterprise Level AWS Services

- Cost Optimization
- Security Strategy
- Best Practice
- Troubleshooting

- Change management
- Network topology
- Association analysis
Splunk Solution
AWS App & Add-on

Splunk App for AWS
Splunk Add-on for AWS
Get Data In
AWS Add-on
Get Data In

- Multi accounts
- Assume Role
- High throughput
- Real-time collection
- Distributed job
- Scale out
- Easy configuration
- Health Monitoring

splunk> Config CloudWatch Kinesis SQS CloudTrail Billing S3 More
### Key New Features in AWS Add-on 4.3 and 4.4

#### New Input: SQS-Based S3

<table>
<thead>
<tr>
<th>CloudTrail</th>
<th>AccessLogs</th>
<th>Config</th>
<th>PlainText</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Event Notification</td>
<td>SQS</td>
<td>Fail over</td>
<td>DLQ</td>
</tr>
</tbody>
</table>

- Higher throughput
- Real-time ingestion
- Cost efficient
- High availability
- Scale out capability
Key New Features in AWS Add-on 4.3 and 4.4

Trouble Shooting: Health Dashboard
Key New Features in AWS Add-on 4.3 and 4.4

Easier Configuration: New Designed Configuration GUI
Best Practice of Get Data In

Example 1: Get CloudTrail Data of Hundreds Accounts in Real-time

- CloudTrail Files: Cross account delivery
- Centralized account
  - S3
    - Bucket 1
    - Bucket 2
    - Bucket 3
- SQS
- S3 event notification
- SQS-Based S3 Input
  - Forwarder 1: Splunk Add-on for AWS
  - Forwarder 2: Splunk Add-on for AWS
  - Forwarder 3: Splunk Add-on for AWS
- Index Cluster
Best Practice of Get Data In
Example 2: Get Data More Securely

EC2 with Instance Role

AssumeRole

Account 1

Account 2

Account 3

Splunk

Config

CloudWatch

CloudTrail

Kinesis

SQS

Billing

S3

Config Rule

Inspector

© 2017 SPLUNK INC.
Data Analysis and Visualization
Key New Features in AWS App 5.1
Reserved Instance Inventory and Planner

- Add support of “Instance Size Flexibility”
Key New Features in AWS App 5.1
Reserved Instance Inventory and Planner

- Add support of “Instance Size Flexibility”

<table>
<thead>
<tr>
<th>Account ID</th>
<th>Region</th>
<th>Platform</th>
<th>Tenancy</th>
<th>Instance type</th>
<th>Existing Rls</th>
<th>Optimal Rls</th>
</tr>
</thead>
<tbody>
<tr>
<td>880758383673</td>
<td>EU (Ireland)</td>
<td>Linux/UNIX</td>
<td>default</td>
<td>c4</td>
<td>48 (unit)</td>
<td>4 (unit)</td>
</tr>
<tr>
<td>880758383673</td>
<td>Asia Pacific (Tokyo)</td>
<td>Linux/UNIX</td>
<td>default</td>
<td>t1</td>
<td>0 (unit)</td>
<td>0.5 (unit)</td>
</tr>
<tr>
<td>880758383673</td>
<td>US West (N. California)</td>
<td>Linux/UNIX</td>
<td>default</td>
<td>t2</td>
<td>5 (unit)</td>
<td>1 (unit)</td>
</tr>
</tbody>
</table>

**Existing Rls:**
You already had 3 reserved instances in this category, converting to unit: 5 = 2 x 2 (medium) + 1 x 1 (small).
- 2 t2.medium with Region scope
- 1 t2.small with Region scope

**Optimal Rls:**
Optimal reserved instances are 1 in unit without considering existing ones.
With instance size flexibility, any combination of instance type from the t2 family can get your RI benefit. For example:
- 1 = 4 x 0.25 (nano)
- 1 = 1 x 1 (small)
Key New Features in AWS App 5.1
Reserved Instance Inventory and Planner

- Add support of **Platform** and **Tenancy** in RI planer
- Support window selection in RI Planer
Key New Features in AWS App 5.1
Anomaly Detection Modular Visualization
Key New Features in AWS App 5.1
Dedicated Dashboard for Anomaly Detection

- Manage anomaly detection jobs
- Manage alerts
- View anomalies detected
Key New Features in AWS App 5.1

More Insights

- IAM
- EIP
- ELB
- COST OPTIMIZING
- EC2
- SECURITY
- EBS
- PERFORMANCE
- SG
- FAULT TOLERANCE
Key New Features in AWS App 5.1

Decoupled Dependency of AWS Add-on

Search Head

- Splunk App for AWS

Forwarder

- Splunk Add-on for AWS

- Not available in hybrid environment
- Not able to connect multiple forwarders
Key New Features in AWS App 5.1

Decoupled Dependency of AWS Add-on

Search Head
Splunk App for AWS

Indexer Cluster
Summary Index

Forwarder
Splunk Add-on for AWS

Forwarder
Splunk Add-on for AWS

Accounts Info
Inputs Info
Typical Use Cases
3 kinds of reports, different granularity

- CloudWatch Estimated Cost
- Monthly Report
- Detailed Billing Report

Budget planning and tracing
Cost analysis on different grouping rules
Cost analysis on customized tags
Case Study – Optimize Reserved Instance

Statistics of RI
- Distribution & utilization
- Detail information

Best purchase plan of RI
- Based on historical data
- Based on forecasting
- Based on adjusted forecasting

Support 3 payment options
Support Regional RI
Support Size Flexibility

Statistics of RI:
- Distribution & utilization
- Detail information

Best purchase plan of RI:
- Based on historical data
- Based on forecasting
- Based on adjusted forecasting

Support options:
- Support 3 payment options
- Support Regional RI
- Support Size Flexibility
Case Study – Topology

Interactive network topology
Interactive IAM association presenting
Export to picture

Multiple overlays
Playback of changes
Case Study – Anomaly Detection

Custom visualization on any time chart

- Number of instance launched daily
- Amount of money spent daily

Native support of alerting

- Email, SNS, ServiceNow
Q&A
Thank You

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