Managing Day-to-day Operations Of Large-scale Splunk Deployment Cost-effectively

Malhar Shah
Crest Data Systems
Disclaimer

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 the 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.
A Day in the Life of a Splunk Admin

Splunk Business Requests:
- Onboarding App Data (Eg: FireEye, WAF, Imperva, Zscaler, Salesforce, AWS, etc.)
- Managing capabilities and assigning Users/groups and roles
- Design Alerts/Dashboards
- Troubleshooting issues
- Training Splunk users

Custom Requirements:
- Index-Time and Search-time field extractions
- Managing custom transforms
- Customizing integrations with 3rd Party Tools
- Building Splunk app for custom home-grown apps

Splunk Infra Management (Splunk Enterprise only):
- Manage Splunk Clustered environment
- Manage/Upgrade Splunk and its Apps/TA/SA
- Storage Management on Indexers
- License Management
- Open LDAP / Active Directory Integration
Customer Topology

**Distributed Splunk Deployment**

- Search Head Deployer
- Search Head Cluster
  - Search Head
  - Search Head
  - Search Head
- License Master
- Deployment Server
- Indexer Cluster
  - Indexer
  - Indexer
  - Indexer
  - Indexer
- Universal Forwarder
- Heavy Forwarder

**Key Elements**

- Distributed Splunk Enterprise Deployment in AWS
- 900+ GB Daily Data Ingestion
- 4,000+ Splunk Forwarders
- 30+ Apps installed
- 5 Indexers
- 3 Search Heads
ServiceNow Integration

**Issue**

- Multiple Alerts are generated across various applications onboarded into Splunk
- Each Event needs be mapped with the application and the entire event details are required to be passed into ServiceNow
- Duplicate tickets need to be checked for a host/source combination and a single unified ticket need to be generated
- The integration requires extensive mapping logic and usage of ServiceNow API

**Solution**

- Mapped each Splunk event field from Splunk with ServiceNow to raise an incident
- Customized Snowcaller was created using Python, which picked up events from Splunk and submitted an incident (to specific business group) in real-time
- Custom logic is implemented to avoid duplicate tickets generation in ServiceNow
Notify Oracle Error Codes to Business Owners

**Issue**
- Several Oracle Error Codes are received on a daily basis
- Customer wants to get notified for all frequently received Error Codes along with minute details of the Error Event so that quick actions can be taken in real-time

**Solution**
- Splunk Admin setup 23 Alerts in Splunk to uniquely identify each ORA Error Code after talking to the Oracle team
- Performed SearchTime extraction of various fields within the Splunk events
  - DBName, HostName, Error Code, Description, Impact/Severity, Environment, Owners, etc.
- Enhanced Logic and correlation was applied to suppress the already received incidents within a given period of time
Optimizing Queries with Data Models

**Issue**

- 80GB data was ingested into a firewall index daily
- This data needed to be sent to a 3rd party tool via Splunk query
- Query took ~4.5 hours to generate results. In some cases the query stopped retrieving results with no output.

**Solution**

- Created a data model for each index and extracted individual fields
- All existing queries were updated using "| tstats with summariseonly = true"
- Started building Data Models in Acceleration Mode with 24 hours of backfill
- Now customer can query current and historically indexed data in seconds
Proactive Best Practices

Infrastructure Advisory
- Design Splunk Architecture on Cloud/On-Prem
- Implement architecture for apps
- Indexer decommissioning and spawning

Splunk Health Monitor
- Rest calls for Splunk downtimes
- Conditional checks to determine missing hosts
- Monitoring via SOS and DMC

License Management
- Alerts to track Daily License Usage
- Identifying explosive host/sources
- Volume Estimation / host / day

Integrations
- Integration with Monitoring Tools such as Big Panda, Zenoss, SiteScope, etc.
- Event Correlations
- Integration with Ticketing tools such as ServiceNow
Best Practices & Cost Effectiveness

<table>
<thead>
<tr>
<th>Reduction in Costs</th>
<th>60%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optimizing the use of hot, warm, and cold storage</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Utilizing storage-saving features of Splunk 6.4</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Setup CIM-compliant Data Models</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Improved Performance</th>
<th>5X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optimizing Data Models by customizing base search, tuning DM acceleration parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Query/Alert optimization, Event correlation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Effective Usage of Deployment Server to manage 4,000+ forwarders</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Average Ticket Age</th>
<th>2 Days</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>24x7 support with Splunk-certified Admins</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Taking quick actions for incoming tickets</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Creating automated ticketing process to involve appropriate business group quickly</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reduction in Incoming Tickets</th>
<th>300%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrations with change management &amp; ticketing tools</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Setup proactive alerts to notify business owners and take corrective actions</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Create Knowledge Base for documenting best practices and issues resolved</strong></td>
<td></td>
</tr>
</tbody>
</table>
Splunk Administrative / Managed Services

Splunk-Certified & Experienced Team Manages All Your Requirements

**Services & Support**
- Manage role-based access control, upgrades, health-check
- Triage issues – ticket and escalation management
- Incident management, Change management

**Architecture Services**
- Review architecture, Optimize performance
- Enable premium solutions such as Enterprise Security, ITSI
- Data archiving and retention

**Integration Services**
- Onboard data from multiple sources
- Build data models, Correlate events, Accelerate reports
- Develop Splunk Apps and Technology Add-ons

**Migration Services**
- Move to AWS or Splunk Cloud
- Migrate from legacy SIEM to Splunk ES
# Splunk Administrative / Managed Services

*Reduce Downtime. Improve Productivity.. Lower TCO...*

<table>
<thead>
<tr>
<th>Certified Admin</th>
<th>24x7 Support</th>
<th>Cost Savings</th>
<th>Flexible Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; Extensive experience in managing Splunk Cloud &amp; Enterprise deployments</td>
<td>&gt; Comprehensive Support from Data Onboarding to Dashboard creation</td>
<td>&gt; 60% reduction in Splunk Administration costs</td>
<td>&gt; 8x5 / 24x5 / 24x7 support options to meet your SLAs</td>
</tr>
<tr>
<td>&gt; Security specialists with SIEM expertise in Splunk Enterprise Security</td>
<td>&gt; Dedicated Admin for each customer</td>
<td>&gt; 20% TCO Reduction on Splunk Cloud</td>
<td>&gt; Hire Part-time or Full-time Administrators</td>
</tr>
<tr>
<td>&gt; Broad experience in IT Ops including ITSI</td>
<td>&gt; Backup admin provided at no additional cost</td>
<td>&gt; 30% TCO Reduction on Splunk Enterprise</td>
<td>&gt; Short-term or Long-term engagement</td>
</tr>
<tr>
<td></td>
<td>&gt; 40+ Splunk Ninjas available globally</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Case Study: Splunk Managed Services (Splunk Enterprise)

*Multi-Billion Dollar NASDAQ-listed Hi-Tech Enterprise*

### Background:
Customer was struggling to keep Splunk Enterprise and Enterprise Security (ES) operational in AWS Cloud
- Frequent outages made it difficult to get desired Operational Intelligence
- Dire need for experienced “Day 2 Ops” team to stabilize and manage Splunk Infrastructure

### Accomplishments in First 90 Days:
- Setup Change Management Process
- Optimized search queries performance by 5X
- Setup ES to monitor 15+ custom Security use cases
- Onboarded 900GB+/day data from 30+ Apps and 4,000+ nodes
- Created custom reports for various Splunk users
- Migrated Splunk Login to AD for Compliance

---

<table>
<thead>
<tr>
<th>Reduction in Admin Costs</th>
<th>Reduction in Splunk TCO</th>
<th>Avg. # Days for Ticket Closure</th>
<th>Reduction in Incoming Tickets</th>
</tr>
</thead>
<tbody>
<tr>
<td>60%</td>
<td>31%</td>
<td>2</td>
<td>20%</td>
</tr>
</tbody>
</table>

“Crest team helped onboard data quickly from several groups across IT. Our teams are gaining more business insights in real-time as a result now.”

Manager, Monitoring, IT Ops
Case Study: Splunk Managed Services (Splunk Cloud)

Multi-Billion Dollar NYSE-listed Hi-Tech Enterprise

Background:
Customer purchased 50GB/day Splunk Cloud license and onboarded a few applications
• Lack of Splunk expertise resulted in obtaining fewer business insights. This sparked internal concerns about Splunk’s value proposition.
• Required onboarding of Premium Apps and Add-ons such as OpenStack which requires customizations

Accomplishments in First 90 Days:
• Onboarded data from 15+ Apps and ~100 nodes
• Developed OpenStack Modules based on custom requirements
• Created custom reports for various Splunk users
• Migrated Splunk Login to AD for Compliance
• Migrated entire infrastructure monitoring to Splunk
• Changed the perception of Splunk by bringing deep operational insights

“Crest went above and beyond their responsibilities to build custom App that brings our OpenStack data into Splunk to deliver never before seen Operational Intelligence through correlations.”
Sr. Manager, IT Ops
THANK YOU

For more information:
info@crestdatasys.com
http://www.crestdatasys.com/