Why and How NHS Digital, the UK’s Health and Social Care Information Centre, Migrated to the Cloud to Reach 7.5TB/Day

Will Searle
Technology Manager | NHS Digital
During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.
Will Searle
Technology Manager | NHS Digital
Agenda
The Journey

1) Where it All Started
   National Monitoring Service

2) Good News Travels Fast
   Further adoption throughout our national services

3) Big-Bang Rapid Adoption
   Removing the bottleneck

4) Regaining Control
   For the greater good

5) Next Steps
   So, what now?
Where it All Started

National Monitoring Service
National Monitoring Service (NMS)
National Monitoring Service

Pros
- Scaled to 100s of users
- Cheap retention (cached results)

Cons
- Lacked newer features
- Management overhead
Good News Travels Fast

Further adoption throughout our national services
How Splunk Spread – Spine 2
Underpinning the monitoring of national services

Launched in 2014

Provides messaging platform between healthcare systems as well as a variety of component services

Became an exemplar service in relation to good monitoring and logging at NHS Digital

Top tip: Establish best practices – For custom logs always include the log level, log reference and a correlation/unique identifier.
How Splunk Spread – Care Identity Service

Underpinning the monitoring of national services

Provides clinical staff secure access to NHS systems

Over 1,000,000 logins per day

Utilises a multisite cluster to record details of every login to support:

• Real-time service monitoring
• Incident Investigation
• Adoption of new features (Self-Service Renewals, Identity Agent upgrades)

Top tip: Plan ahead and reduce tech-debt by doing it right early on. Search for ”Splunk Validated Architectures”.

Big-Bang Rapid Adoptions

Removing the bottleneck
How the Use of Splunk Spread

More services, different use-cases, new users

Security
Scale-out of our Security Operations Centre (SOC)

DevOps
Increased utilization of Splunk in DevOps environments

Common Skills
Staff from areas already using Splunk moving around

Programmes
New programmes followed proven patterns
Single Toolset for Multiple Purposes

Provides a single place to look, regardless of the task:
Single Toolset for Multiple Purposes

Provides a single place to look, regardless of the task:

- Operational Support
Single Toolset for Multiple Purposes

Provides a single place to look, regardless of the task:

• Operational Support
• Incident Investigation
Single Toolset for Multiple Purposes

Provides a single place to look, regardless of the task:

• Operational Support
• Incident Investigation
• Development Lifecycle
Single Toolset for Multiple Purposes

Provides a single place to look, regardless of the task:

- Operational Support
- Incident Investigation
- Development Lifecycle
- Security Monitoring
Single Toolset for Multiple Purposes

Provides a single place to look, regardless of the task:

• Operational Support
• Incident Investigation
• Development Lifecycle
• Security Monitoring
• Service Management
Single Toolset for Multiple Purposes

Provides a single place to look, regardless of the task:

- Operational Support
- Incident Investigation
- Development Lifecycle
- Security Monitoring
- Service Management
- Executive summary
The Pitfalls of Rapid Growth

No ability to search across instances
The Pitfalls of Rapid Growth

No ability to search across instances

Lots of dark data
The Pitfalls of Rapid Growth

No ability to search across instances

Lots of dark data

Security and Patching
The Pitfalls of Rapid Growth

No ability to search across instances
Lots of dark data
Security and Patching
Economy of scale
The Pitfalls of Rapid Growth

No ability to search across instances
Lots of dark data
Security and Patching
Economy of scale
Lack of best practice
The Pitfalls of Rapid Growth

No ability to search across instances
Lots of dark data
Security and Patching
Economy of scale
Lack of best practice
Governance
We Couldn’t See the Forest, or the Trees

Instances
75+ Individual deployments

Support
Unsupported versions (<7.x)

Maturity
Wide range of maturity

Approach
Inconsistent approach

Planning
Difficulty of forecasting future requirements
Regaining Control
For the greater good
Step 1 – No More License Keys

Cloud-first
Low maintenance
Simple reporting
Reaching for the Sky (Cloud)
A fresh start
Reaching for the Sky (Cloud)
A fresh start

Create a plan
Reaching for the Sky (Cloud)

A fresh start

Create a plan

Consolidate efforts
Reaching for the Sky (Cloud)

A fresh start

Create a plan

Consolidate efforts

Training – All on the same page
Reaching for the Sky (Cloud)

A fresh start

Create a plan

Consolidate efforts

Training – All on the same page

Admin on Demand
Reaching for the Sky (Cloud)
A fresh start

Create a plan
Consolidate efforts
Training – All on the same page
Admin on Demand
Maximising the Splunk Investment
Reaching for the Sky (Cloud)

A fresh start

Create a plan

Consolidate efforts

Training – All on the same page

Admin on Demand

Maximising the Splunk Investment

Reduces Total Cost of Ownership (TCO)
Managing a Splunk deployment involves 12 on-going admin tasks, 8 of which are conducted by Splunk for a Cloud based deployment.

### On-Premise vs. Splunk Cloud

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Splunk Ent Deployed On-Premises</th>
<th>Splunk Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Tasks: One-time Setup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase/rent HW</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Rack and stack, cable, network all HW</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Install Splunk</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Install OS</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Configure Splunk (create users, load apps, configure)</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Configure indexes</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Setup HA/clustering</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Setup disaster and recovery</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Configure forwarders</td>
<td>Customer</td>
<td>Joint</td>
</tr>
<tr>
<td>Onboard data</td>
<td>Customer</td>
<td>Joint</td>
</tr>
<tr>
<td>Integrate with LDAP/AD</td>
<td>Customer</td>
<td>Joint</td>
</tr>
<tr>
<td>Admin Tasks: Ongoing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scale up HW</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Install Splunk patches / upgrades</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Install OS patches / upgrades</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Monitor deployment / health checks</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Manage forwarders</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Create users / roles</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Manage indexes</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Onboard additional data</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Load search head only apps</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Load distributed apps</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Load premium apps</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>Export data</td>
<td>Customer</td>
<td>Splunk</td>
</tr>
<tr>
<td>User Tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search, alerts, reports, dashboards</td>
<td>Customer</td>
<td>Customer</td>
</tr>
</tbody>
</table>
What is Cost?

“The effort, loss, or sacrifice necessary to achieve or obtain something” (Oxford Living Dictionary, 2019)

Cost isn’t just monetary:

1. Risk
2. Opportunity
3. Innovation
4. Environmental
5. Quality

Why Splunk Cloud?
How Things Look Now

300+ Indexes
500+ Active Users
700+ Sourcetypes
100k+ Sources
Next Steps

So, what now?
12 Month Plan

Reuse, Reuse, Reuse

Consolidation

Improve Maturity
1. Top Tips
   • For custom logs always include the log level, log reference and a unique identifier
   • Plan ahead and reduce tech-debt by doing it right early on

2. Avoid creating data silos

3. Sweat the asset

4. Create a roadmap (and follow it!)
Thank You

Please provide feedback via the SESSION SURVEY