Bringing Sweetness to Sour Patch Tuesday

Pacific Northwest National Laboratory

Justin Brown & Arzu Gosney

September 27, 2017 | Washington, DC
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. © 2017 Splunk Inc. All rights reserved.
About Me

- IT Engineer
- Technical Lead
- Automation & Monitoring Team
- Joined PNNL in 2000

Arzu Gosney
Arzu.Gosney@pnnl.gov
@ArzuGosney
About PNNL
(Pacific Northwest National Laboratory)
Agenda

- Where We Were
  - Problem description
  - Goals

- Where We Are Now
  - Current process demonstration
  - Explaining Why

- How We Did It
  - Key Components
  - Writing queries
  - Building dashboards
Where We Were

The Problems with Patch Week

Goals for Improvement
Where We Were

The Problems with Patch Week

► Slow problem discovery
  • Failed patches
  • Multiple reboots
  • False positives

► Manual Processes
  • Servers checked in SCOM, SCCM, Splunk, manually
  • Applications checked manually (SharePoint checklist)
  • Resource intensive
<table>
<thead>
<tr>
<th>IT Service</th>
<th>Current Hour</th>
<th>Past 24 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SharePoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring (Synthetic Trans)</td>
<td>![Green Checkmark]</td>
<td>![Caution]</td>
</tr>
<tr>
<td>DATE</td>
<td>STATUS</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>04/26/2016 - 01:46:31 AM</td>
<td>Closed</td>
<td></td>
</tr>
<tr>
<td>04/25/2016 - 10:36:31 PM</td>
<td>Closed</td>
<td></td>
</tr>
<tr>
<td>04/25/2016 - 03:17:12 PM</td>
<td>Closed</td>
<td></td>
</tr>
</tbody>
</table>

**Links**
- Maximo: DOM Start Center
- Forward Schedule of Change
- Changes Not As Planned
- OIM Agenda
- Website Visitors Dashboard
- DOM Dashboard Information & Instructions
- Monitoring & Automation Team Blog

**Subject**

<table>
<thead>
<tr>
<th>Status</th>
<th>From</th>
<th>Updated</th>
</tr>
</thead>
</table>

No status updates have been submitted today.
Where We Were

Goals for Improvement

- Patching status for all Windows servers
  - Drilldown for individual server details
  - Dashboard for patches by status

- Web Application health dashboard
  - Rollup of website and database monitoring

- Automated Reports & Alerts
  - Reports emailed to teams with status
  - Alerts sent to incident responders
Where We Are Now

Current Process Demonstration
Explaining Why
## IT - Platform Services - Host Patching Status

**Server Info:** amor

<table>
<thead>
<tr>
<th>Server</th>
<th>Operating System</th>
<th>Online</th>
<th>Patched</th>
<th>Restarted</th>
<th>Reboots</th>
<th>Last Seen</th>
<th>Last Restart</th>
<th>Updates Detected</th>
<th>Installed</th>
<th>Failed</th>
<th>Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>amor</td>
<td>Microsoft Hyper-V Server 2012 R2</td>
<td>❌</td>
<td>✅</td>
<td>2</td>
<td>2</td>
<td>04/26/2016 - 05:21:01 AM</td>
<td>04/18/2016 - 10:28:50 AM</td>
<td>9</td>
<td>7</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

### Patch Details

<table>
<thead>
<tr>
<th>Update</th>
<th>Status</th>
<th>Latest Attempt</th>
<th>Success Count</th>
<th>Fail Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Update for Microsoft Silverlight (KB3120503)</td>
<td>Failed</td>
<td>04/25/2016 - 09:31:54 PM</td>
<td>0</td>
<td>117</td>
</tr>
<tr>
<td>Update for Forefront Endpoint Protection 2010 Client - 4.9.218.0 (KB3106243)</td>
<td>Failed</td>
<td>04/25/2016 - 09:31:54 PM</td>
<td>0</td>
<td>117</td>
</tr>
<tr>
<td>Security Update for Windows Server 2012 R2 (KB3134596)</td>
<td>Patched</td>
<td>04/18/2016 - 10:14:51 AM</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Security Update for Windows Server 2012 R2 (KB3173705)</td>
<td>Patched</td>
<td>04/18/2016 - 10:14:51 AM</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Security Update for Windows Server 2012 R2 (KB3846716)</td>
<td>Patched</td>
<td>04/18/2016 - 10:14:51 AM</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Security Update for Windows Server 2012 R2 (KB3846723)</td>
<td>Patched</td>
<td>04/18/2016 - 10:14:51 AM</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Security Update for Windows Server 2012 R2 (KB3846963)</td>
<td>Patched</td>
<td>04/17/2016 - 07:00:49 AM</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Security Update for Windows Server 2012 R2 (KB3847002)</td>
<td>Patched</td>
<td>04/18/2016 - 10:14:51 AM</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Update for Windows Server 2012 R2 (KB3399023)</td>
<td>Patched</td>
<td>04/18/2016 - 10:14:51 AM</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
## IT - Platform Services - Patch Report

**Status**

- Failed

**Patches with status: Failed**

<table>
<thead>
<tr>
<th>update</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>April, 2017 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014985)</td>
<td>11</td>
</tr>
<tr>
<td>Security Update for Microsoft Silverlight (KB4017004)</td>
<td>4</td>
</tr>
<tr>
<td>April, 2017 Security Only Update for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014988)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB4014987)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014984)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014981)</td>
<td>2</td>
</tr>
<tr>
<td>October, 2016 Security Only Update for .NET Framework 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 (KB3188736)</td>
<td>2</td>
</tr>
<tr>
<td>Update for Microsoft Visual Studio 2010 Tools for Office Runtime (KB2961149)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4015549)</td>
<td>1</td>
</tr>
<tr>
<td>Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB29900986)</td>
<td>1</td>
</tr>
<tr>
<td>Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4014561)</td>
<td>1</td>
</tr>
<tr>
<td>Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB3124275)</td>
<td>1</td>
</tr>
</tbody>
</table>
## Application Dashboard

Provide a check list for applications with and without synthetic transaction

### Application Check List

<table>
<thead>
<tr>
<th>Department</th>
<th>Application</th>
<th>Details</th>
<th>Criticality</th>
<th>Status</th>
<th>Notes</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Platform Management</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Platform Management</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Filter Status:** All
- **Criticality Filter:** All
- **Filter Warnings/fails:** All

**Reset**
<table>
<thead>
<tr>
<th>Department</th>
<th>Application</th>
<th>Details</th>
<th>Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Platform</td>
<td>Management</td>
<td></td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security and Health</td>
<td>4</td>
<td></td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security and Health</td>
<td>5</td>
<td></td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security and Health</td>
<td>4</td>
<td></td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Environmental, Safety, Security and Health</td>
<td>5</td>
<td></td>
<td>Passed</td>
<td></td>
</tr>
</tbody>
</table>

Lasted Tested by: [Name] on 04/16/17 01:05 PM
Where We Are Now
Explaining Why

- Centralized Reports
- Centralized Management Interfaces
- Centralized Alerts
- Time Savings
Where We Are Now

Time Savings

Time Savings on Patch Dashboard

Savings in Hours & Dollars by Fiscal Year

<table>
<thead>
<tr>
<th>FY</th>
<th>Savings in Hours</th>
<th>Savings in Dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>'16</td>
<td>221.98</td>
<td>635.38</td>
</tr>
<tr>
<td>'17</td>
<td>19,534.24</td>
<td>57,673.44</td>
</tr>
</tbody>
</table>

Total Raw Hours Saved Since FY15

877

Total Raw Hour Dollar Savings Since FY15

$77,207.68
How We Did It

Key Components
Writing Queries
Building Dashboards
About Me

▶ IT Engineer
▶ Splunk Technical Lead
▶ Automation & Monitoring Team
▶ Joined PNNL in 2000

Justin Brown
justin@pnnl.gov
@theOtherJustinB
Key Components

Splunk

- All of our data in one place
- Reporting and visualization tools
- Monitoring and alerting capabilities
- Custom development features
Key Components

WLS (Windows Logging Service)

- Windows Logging Service (WLS)
  - Developed by Jason McCord at Kansas City National Security Campus
  - [https://digirati82.com/wls-information](https://digirati82.com/wls-information)

- Certificates
- Devices
- Drives
- File metadata
- File system changes
- Loaded Modules
- Named Pipes
- Performance Counters
- Port Monitoring
- Registry Changes
- Windows Objects
- WMI Queries
Key Components
Other Data Sources

- SCOM Alerts
- Universal Forwarder
  - IIS logs
- DBConnect
  - https://splunkbase.splunk.com/app/2686/
  - Database Connection testing
WARNING!
Writing the Queries

Things we need to know

- Is it patched?
  - False positives?
- Are there patches pending?
- Have patches failed?
- Has it rebooted?
  - Multiple times?
- Is it online?
Writing the Queries
Getting Patch Status from Windows Events

▶ Updates Downloaded or Pending
  • EventID 18
  • EventID 41 or 44 (Windows Server 2016)

▶ Update Installation Events
  • EventID 19 – Success
  • EventID 20 – Failed

▶ Install Complete – Reboot Pending
  • EventID 21 or 22

▶ Event Collection Note
  • If you are using WLS, turn on the Backfill option
Writing the Queries

Detecting Reboots

Using Windows Event Logs
- Event ID 6005 indicates start up

Using WMI queries in WLS
- Collected every hour or on reboot
- Includes last boot up time

```
source=wls:wmi OperatingSystem
```
Writing the Queries

Narrowing results to just servers

Servers seen online in the last 30 days

```bash
source=wls:wmi OperatingSystem ProductTypeType>1
| dedup host | table host, Caption | rename Caption as os
| outputlookup windows_servers_discovered
```

Servers online recently

- Splunk keeps track of which systems are sending data
- WLS sends updates at least every five minutes

```bash
| inputlookup windows_servers_discovered
| join host [ | metadata type=hosts index=os
| where lastTime > relative_time(now(), "-2h") | fields host]
| outputlookup windows_servers_online
```
Writing the Queries
 Putting it all together

index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updateTitle NOT "EventID=\"17\"" NOT "EventID=\"43\"" NOT "Definition Update"
 | inputlookup windows_servers_online | fields host
 | appendpipe
 | | search updatelist=* | stats latest(updatelist) as updatelist, latest(_time) as _time by host, EventID
 | | makemv delim=;" updatelist
 | | eval updateTitle = ltrim(updatelist,-")
 | rex field=updateTitle "^(?<update>\[\{\}\]+(\+[\{]KB\d+))"
 | append [] inputlookup windows_servers_online.csv | fields host | eval update="No Updates Found"
 | stats count(eval(EventID=19)) as install_primary,
 | count(eval(EventID=21 OR EventID=22)) as install_backup,
 | max(eval(if(EventID=19 OR EventID=21 OR EventID=22,_time,NULL))) as latest_install,
 | count(eval(EventID=20)) as fail_count,
 | max(eval(if(EventID=20,_time,NULL))) as latest_fail,
 | max(eval(if((EventID==21 OR EventID==22),_time,NULL))) as latest_reboot_pending by host, update
 | join type=left host
 | | search index=os source=wls:wmi OperatingSystem [] inputlookup windows_servers_online.csv | fields host
 | | addinfo
 | | eval last_restart = strptime(LastBootUpTime,"%Y%m%d%H%M%S\.%f")
 | | stats latest(Caption) as os,
 | | max(last_restart) as last_restart,
 | | dc(eval(if(last_restart > info_min_time,last_restart,NULL))) as restart_count by host
 | | eval pending_reboot = if(latest_reboot_pending > last_restart, 1, 0)
 | | eval install_count = if(install_primary==0,install_backup,install_primary)
 | | join type=left host
 | | | metadata type=hosts index=os | fields host, lastTime
 | | | eval online=if(lastTime > relative_time(now(),"-60m"),1,0)
 | | | eventstats count(eval(update!="No Updates Found")) as real_updates by host
 | | | search real_updates=0 OR update!="No Updates Found"
 | | | eval patch_status = case(real_updates==0, 1, install_count > 2, 3, install_count > 0,0, fail_count == 0, 2, fail_count > 0, 4)
Writing the Queries

Breaking it down

```plaintext
index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updateTitle NOT "EventID="17"" NOT "EventID="43"" NOT "Definition Update"
  || inputlookup windows_servers_online | fields host]
| appendpipe
  || search updatelist=* ||
  | stats latest(updatelist) as updatelist, latest(_time) as _time by host, EventID
  | makemv delim=";" updatelist
  | eval updateTitle = ltrim(updatelist,"- ")
| rex field=updateTitle "^(?<update>[^\(]+\(KB\d+)\))"
| append
  || inputlookup windows_servers_online.csv
  | fields host
  | eval update="No Updates Found"
```
## Writing the Queries

### Breaking it down

<table>
<thead>
<tr>
<th>_time</th>
<th>host</th>
<th>EventID</th>
<th>updatelist</th>
<th>updateTitle</th>
<th>update</th>
</tr>
</thead>
</table>
Search Tip

Searching raw text is faster than non-indexed fields

```
index=os ProviderName="Microsoft-Windows-WindowsUpdateClient" updateList=* OR updateTitle=* NOT EventID=17 NOT EventID=43
| inputlookup windows_servers_online.csv | fields _time, host, EventID, updateList, updateTitle
| appendpipe
|    | stats latest(updateList) as updateList, latest(_time) as _time by host, EventID
|    | makemv delim="," updateList
|    | eval updateTitle = ltrim(updateList," ").*
|    | rex field=updateTitle "^[?update>[^\|\(\}\]\{\(\{\)\}\)]"
|    | inputlookup windows_servers_online.csv append=t
| append pipe windows_servers_online.csv
```

48,120 events (7/11/17 12:00:00.000 AM to 7/25/17 12:00:00.000 AM) No Event Sampling

Search job inspector

This search has completed and has returned 80,497 results by scanning 5,801,048 events in 554.121 seconds
(SID: 1502232189:1705199) search.log
Search Tip

Searching raw text is faster than non-indexed fields

```
index=os ProviderName="Microsoft-Windows-WindowsUpdateClient" updatelist=* OR updateTitle=* NOT EventID=17 NOT EventID=43
```

```
index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updateTitle NOT "EventID="17" NOT "EventID="43"
```
Search Tip

Searching raw text is faster than non-indexed fields

Before

Search job inspector

This search has completed and has returned 50,497 results by scanning 5,801,048 events in 554.121 seconds
(SID: 1502232189.1705199) search.log

After

Search job inspector

This search has completed and has returned 50,497 results by scanning 77,544 events in 85.945 seconds
(SID: 1502233019.1705940) search.log
Writing the Queries
Breaking it down

| stats count(eval(EventID=19)) as install_primary, count(eval(EventID=21 OR EventID=22)) as install_backup, max(eval(if(EventID=19 OR EventID=21 OR EventID=22,_time,NULL))) as latest_install, count(eval(EventID=20)) as fail_count, max(eval(if(EventID=20,_time,NULL))) as latest_fail, max(eval(if((EventID==21 OR EventID==22),_time,NULL))) as latest_reboot_pending by host, update
## Writing the Queries

### Breaking it down

<table>
<thead>
<tr>
<th>host</th>
<th>update</th>
<th>install_primary</th>
<th>install_backup</th>
<th>latest_install</th>
<th>fail_count</th>
<th>latest_fail</th>
<th>latest_reboot_pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>sample1</td>
<td>No Updates Found</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sample2</td>
<td>2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)</td>
<td>3</td>
<td>1</td>
<td>1505325478</td>
<td>0</td>
<td></td>
<td>1505317194</td>
</tr>
<tr>
<td>sample2</td>
<td>2017-09 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4038793)</td>
<td>1</td>
<td>1</td>
<td>1505324961</td>
<td>0</td>
<td></td>
<td>1505317194</td>
</tr>
<tr>
<td>sample2</td>
<td>2017-09 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 8.1 and Server 2012 R2 for x64 (KB4041092)</td>
<td>1</td>
<td>1</td>
<td>1505324961</td>
<td>0</td>
<td></td>
<td>1505317194</td>
</tr>
<tr>
<td>sample2</td>
<td>Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4036586)</td>
<td>1</td>
<td>1</td>
<td>1505324962</td>
<td>0</td>
<td></td>
<td>1505317194</td>
</tr>
<tr>
<td>sample2</td>
<td>Update for Windows Server 2012 R2 (KB4033428)</td>
<td>1</td>
<td>1</td>
<td>1505324961</td>
<td>0</td>
<td></td>
<td>1505317194</td>
</tr>
<tr>
<td>sample2</td>
<td>No Updates Found</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sample3</td>
<td>2017-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4034664)</td>
<td>1</td>
<td>1</td>
<td>1505400183</td>
<td>0</td>
<td></td>
<td>1505399639</td>
</tr>
<tr>
<td>sample3</td>
<td>2017-09 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4038779)</td>
<td>0</td>
<td>0</td>
<td></td>
<td>1</td>
<td>1505399639</td>
<td></td>
</tr>
<tr>
<td>sample3</td>
<td>2017-09 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 7 and Server 2008 R2 for x64 (KB4041090)</td>
<td>1</td>
<td>1</td>
<td>1505400183</td>
<td>0</td>
<td></td>
<td>1505399639</td>
</tr>
<tr>
<td>sample3</td>
<td>2017-09 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 7 and Server 2008 R2 for x64 (KB4041083)</td>
<td>1</td>
<td>1</td>
<td>1505400183</td>
<td>0</td>
<td></td>
<td>1505399639</td>
</tr>
<tr>
<td>sample3</td>
<td>Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB4036586)</td>
<td>1</td>
<td>1</td>
<td>1505400183</td>
<td>0</td>
<td></td>
<td>1505399639</td>
</tr>
<tr>
<td>sample3</td>
<td>No Updates Found</td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| join type=left host
| [ search index=os source=wls:wmi OperatingSystem [ | inputlookup windows_servers_online.csv | fields host]
| addinfo | eval last_restart = strptime(LastBootUpTime,"%Y%m%d%H%M%S.%f")
| stats latest(Caption) as os,
| max(last_restart) as last_restart,
| dc(eval(if(last_restart > info_min_time, last_restart, NULL))) as restart_count
| by host]
Writing the Queries

Breaking it down

```eval
| eval pending_reboot = if(latest_reboot_pending > last_restart, 1, 0)
| eval install_count = if(install_primary==0,install_backup,install_primary)
| join type=left host
    [ | metadata type=hosts index=os | fields host, lastTime]
| eval online = if(lastTime > relative_time(now(),"-60m"),1,0)
| eventstats count(eval(update!="No Updates Found")) as real_updates by host
| search real_updates=0 OR update!="No Updates Found"
| eval patch_status = case(
    real_updates == 0, 1,
    install_count > 2, 3,
    install_count > 0, 0,
    fail_count == 0, 2,
    fail_count > 0, 4)
```
### Writing the Queries

#### Breaking it down

<table>
<thead>
<tr>
<th>host</th>
<th>update</th>
<th>install_primary</th>
<th>install_backup</th>
<th>install_count</th>
</tr>
</thead>
<tbody>
<tr>
<td>sample1</td>
<td>No Updates Found</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>sample2</td>
<td>2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sample2</td>
<td>2017-09 Security Update for Adobe Flash Player for Windows Server 2012 R2 for x64-based Systems (KB4038806)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sample2</td>
<td>2017-09 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 8.1 and Server 2012 R2 for x64 (KB4041085)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sample2</td>
<td>Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4036586)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sample2</td>
<td>Update for Windows Server 2012 R2 (KB4033428)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sample3</td>
<td>2017-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4034664)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>sample3</td>
<td>2017-09 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4038779)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Search Tip

Using the LOADJOB command

```
index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updatelist NOT "EventID="17"" NOT "EventID="43"
[] inputlookup windows_servers_online.csv | fields host
| fields _time, host, EventID, updatelist, updatelist
| appendpipe
| [] stats latest(updatelist) as updatelist, latest(_time) as _time by host, EventID
| | makecsv delims="" updatelist
| | eval updateTitle = ltrim(updatelist,"- ") ]
| rex field=updateTitle "^(?<update>[\w]+)(KB\d\d)"
| inputlookup windows_servers_online.csv appendl
| fillnull value="No Updates Found" update
```

Search job inspector

This search has completed and has returned 50,497 results by scanning 77,544 events in 85.945 seconds

(SID: 1502233019.1705940) search.log
Search Tip
Using the LOADJOB command
## IT - Platform Services - Patch Report

### Patches with status: Failed

<table>
<thead>
<tr>
<th>update</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>April, 2017 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014985)</td>
<td>11</td>
</tr>
<tr>
<td>Security Update for Microsoft Silverlight (KB4017094)</td>
<td>4</td>
</tr>
<tr>
<td>April, 2017 Security Only Update for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014988)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB4014987)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014984)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014981)</td>
<td>2</td>
</tr>
<tr>
<td>October, 2016 Security Only Update for .NET Framework 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 (KB3188736)</td>
<td>2</td>
</tr>
<tr>
<td>Update for Microsoft Visual Studio 2010 Tools for Office Runtime (KB2961149)</td>
<td>2</td>
</tr>
<tr>
<td>April, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4015543)</td>
<td>1</td>
</tr>
<tr>
<td>Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB25900986)</td>
<td>1</td>
</tr>
<tr>
<td>Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4014661)</td>
<td>1</td>
</tr>
<tr>
<td>Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB3124275)</td>
<td>1</td>
</tr>
</tbody>
</table>
Building the Dashboards
Use Base Searches

<form script="server_status.js" stylesheet="server_status.css" refresh="600">
<label>IT - Platform Services - Server Monitoring for Patch Weekend</label>
<search id="monitoring" ref="patch_monitoring_report"></search>
Building the Dashboards

Custom Icons

<form script="server_status.js" stylesheet="server_status.css" refresh="600">
<label>IT - Platform Services - Server Monitoring for Patch Weekend</label>
<search id="monitoring" ref="patch_monitoring_report"></search>

▶ File location:
• $SPLUNK_HOME$/etc/apps/<your app name>/appserver/static
Building the Dashboards

Custom Icons

server_status.js

```javascript
require(['underscore', 'jquery', 'splunkjs/mvc', 'splunkjs/mvc/tableview', 'splunkjs/mvc/simplexml/ready!'], function(_, $, mvc, tableView) {

  var ICONS = {
    0: 'box-filled',
    1: 'box-filled',
    2: 'box-filled',
    3: 'alert',
    4: 'box-filled'
  };

  var TITLES = {
    'Patched': {
      0: 'All Patches Installed!',
      1: 'No patches detected',
      2: 'Patches detected and pending install',
      3: 'An individual patch has "successfully" installed multiple times',
      4: 'One or more patches have failed to install'
    },
    'Critical': {
      0: 'Critical!',
      1: 'Still critical',
      2: 'No critical messages',
      3: 'One or more critical messages'
    }
  };
```

One or more patches have failed to install
```javascript
require([],
  'underscore',
  'jquery',
  'splunkjs/mvc',
  'splunkjs/mvc/tableview',
  'splunkjs/mvc/simplexml/ready!'
], function(_, $, mvc, TableView) {

  var ICONS = {
    0: 'box-filled',
    1: 'box-filled',
    2: 'box-filled',
    3: 'alert',
    4: 'box-filled'
  }

  var TITLES = {
    'Patched': {
      0: 'All Patches Installed!',
      1: 'No patches detected',
      2: 'Patches detected and pending install',
      3: 'An individual patch has "successfully" installed multiple times',
      4: 'One or more patches have failed to install'
    },
    'Online': {
      0: 'Server is regularly checking in'
    }
  }
```
```
```javascript
var RangeMapIconRenderer = TableView.BaseCellRenderer.extend({
  canRender: function(cell) {
    return cell.field === 'Restarted' || cell.field === 'Patched' || cell.field === 'Online';
  },

  render: function($td, cell) {
    var icon = 'question';
    if (ICONS.hasOwnProperty(cell.value)) {
      icon = ICONS[cell.value];
    }

    var title = 'Unknown Status';
    if (TITLES.hasOwnProperty(cell.field)) {
      title = TITLES[cell.field][cell.value];
    }

    $td.addClass('icon').html(_template('<i class="icon-%s icon" level=%s range %s title=%s title "%s"></i>', {
      icon: icon,
      range: cell.value,
      title: title
    }));
  }
});

mvc.Components.get('Status').getVisualization(function(tableView){
  tableView.table.addCellRenderer(new RangeMapIconRenderer());
  tableView.table.render();
});
```
Building the Dashboards

Set the ID of the table

```xml
<row>
  <panel>
    <title>Server Details</title>
    <table id="Status">
      <title>Includes Windows 2008 &amp; 2012 Servers</title>
      <search base="monitoring">
        ....
      </search>
    </table>
  </panel>
</row>
```
Building the Dashboards

Custom Icons

Before

After
Alert Tip

Send **multiple emails** to **different recipients** using lookups

<table>
<thead>
<tr>
<th>host</th>
<th>contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>sample1</td>
<td><a href="mailto:admin1@sample.email">admin1@sample.email</a></td>
</tr>
<tr>
<td>sample2</td>
<td><a href="mailto:admin2@sample.email">admin2@sample.email</a></td>
</tr>
<tr>
<td>sample3</td>
<td><a href="mailto:admin3@sample.email">admin3@sample.email</a></td>
</tr>
<tr>
<td>sample4</td>
<td><a href="mailto:admin4@sample.email">admin4@sample.email</a></td>
</tr>
<tr>
<td>sample5</td>
<td><a href="mailto:admin5@sample.email">admin5@sample.email</a></td>
</tr>
<tr>
<td>sample6</td>
<td><a href="mailto:admin6@sample.email">admin6@sample.email</a></td>
</tr>
<tr>
<td>sample7</td>
<td><a href="mailto:admin7@sample.email">admin7@sample.email</a></td>
</tr>
</tbody>
</table>
Summary
Everything from a single report

• Dashboards
  • Patching Progress Status
  • Server details
  • Patch details

• Reports
  • Schedule reports for specific groups of servers
  • Full status report

• Alerts
  • Notify specific teams if servers aren’t patched
Thank You

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