splunk> .conf2017

SELF ADAPTING OPS DASHBOARDS

Office of Information Technology Services

Barry Krawchuk | Research Scientist

September 25, 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.

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

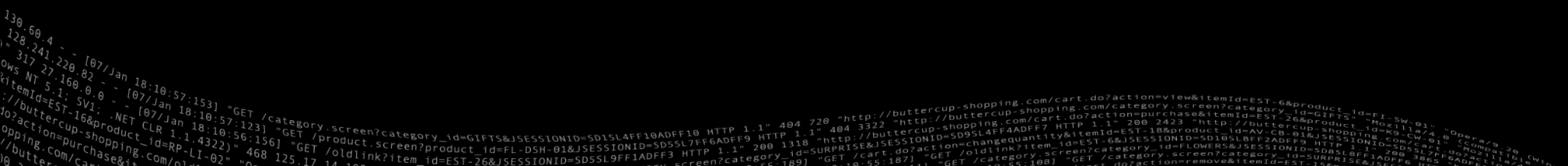
splunk> .conf2017

Information Technology Services

New York State

- Integration of NYS Information Technology
  - 55 State Agencies
  - 10,000 Servers
  - 144,000 Employees

"A computer lover's heaven with every kind of software and computer you could ever want"



NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

splunk> .conf2017

“It’s a Love Hate Relationship.”

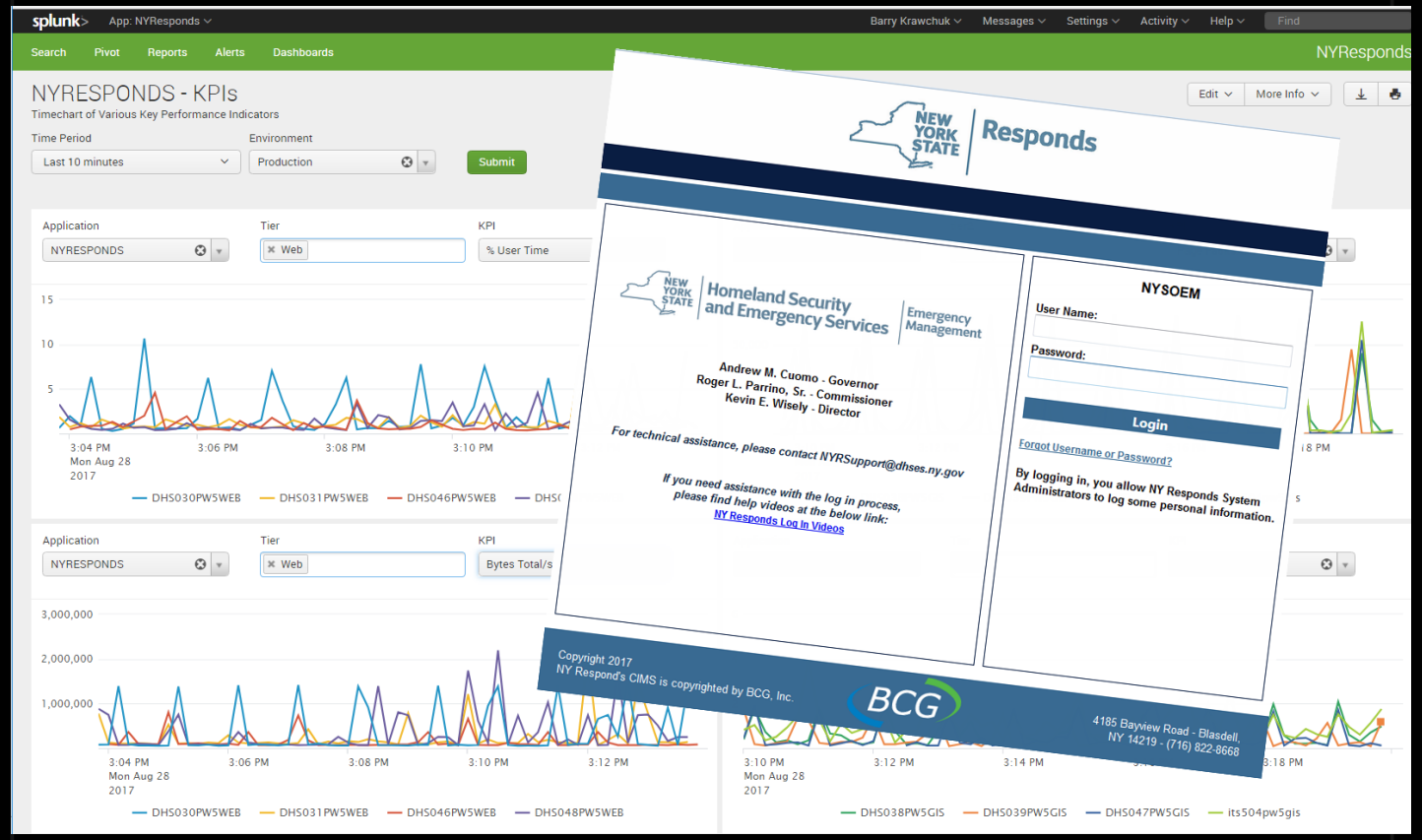
A voice in the corner of the office

NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

splunk> .conf2017

Who Asks For Splunk Services?

Statewide Disaster Response and Management



- Performance KPIs
  - Heavy load testing
  - Available 24 x 7
- Environments
  - Production
  - QA
- Tiers
  - GIS
  - Application
  - Web

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Who Asks For Splunk Services?

NYS Integrated Justice Information Portal

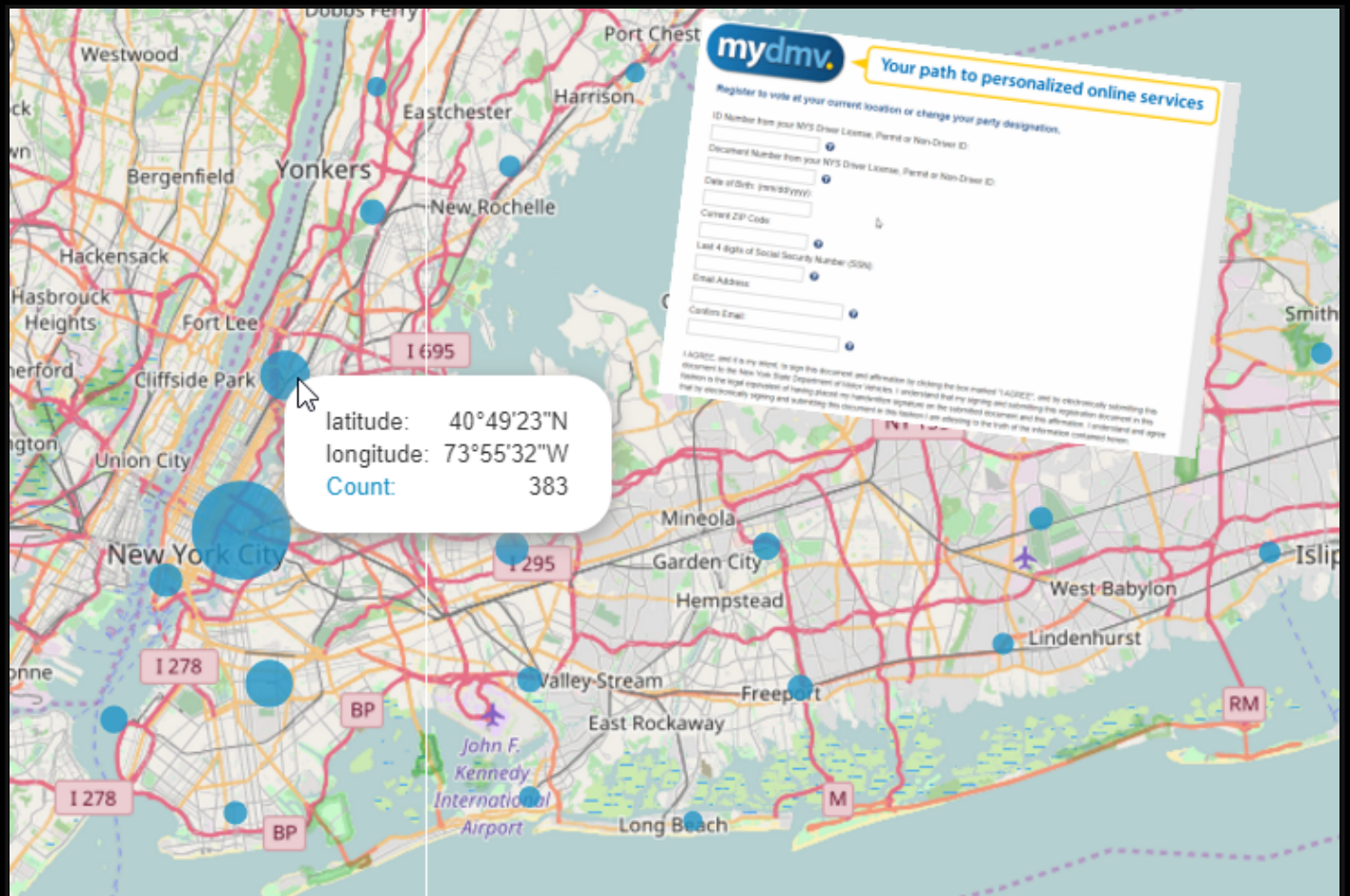
- Performance KPIs
- Errors and Usage
- Environments
  - 67 hosts
  - PROD, QA & DEV
- Tiers
  - datapower, ftp, mail
  - mq, was, wbm, wpo, wps
  - web

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Who Asks For Splunk Services?

Voter Registration – Rapid to Market



- Performance KPIs
  - Crucial Load Tests
  - Continuous Monitoring
  - Business Results
- Environments
  - PROD, QA, DEV
- Tiers
  - App, FS, SQL, WEB

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Information Technology Systems

Splunk Team

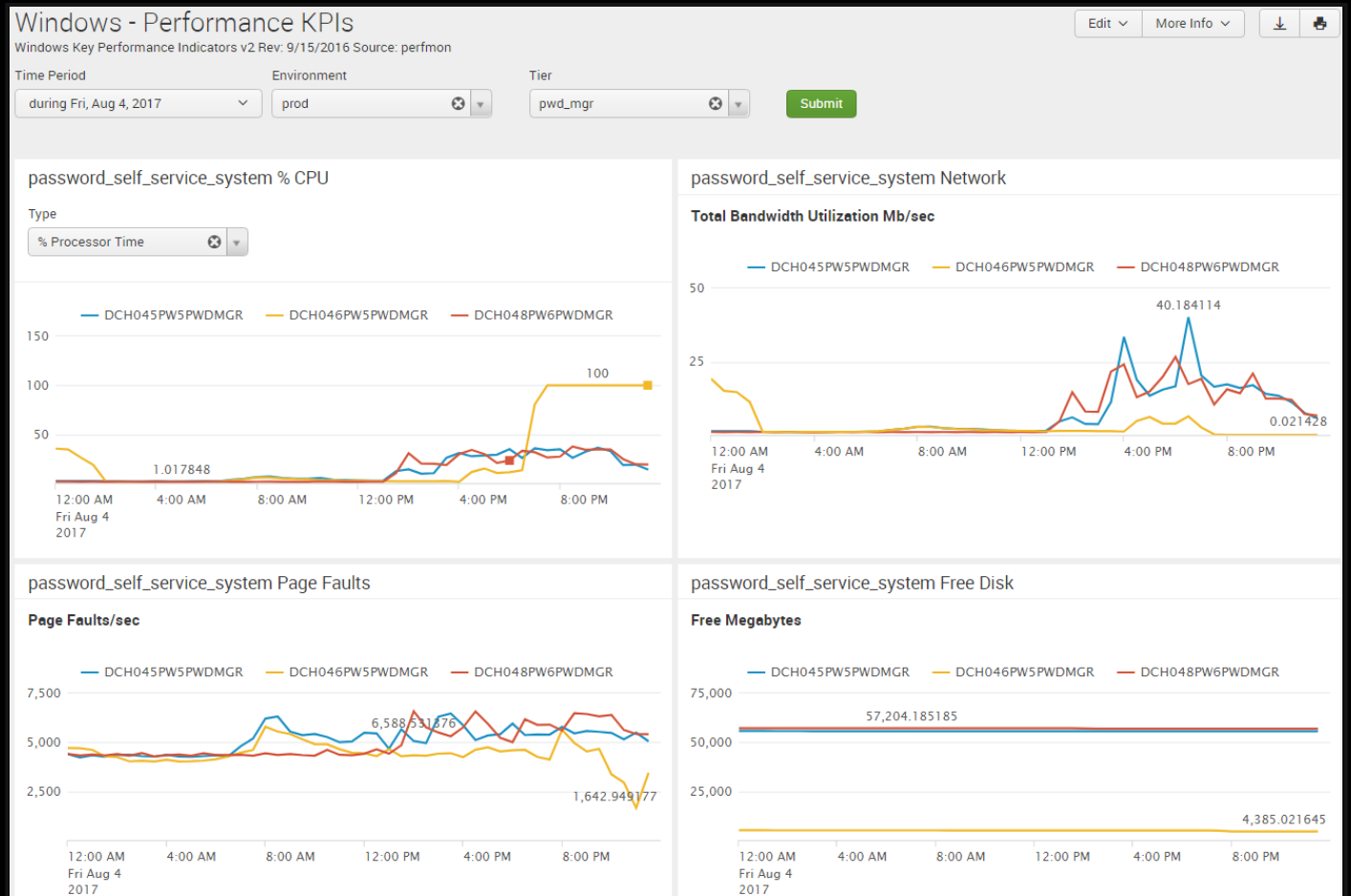
- By now it should be clear:
  - NYS has a large demand for Splunk Services
    - Many agencies, many applications
    - Critical business delivery requirements
    - Streamlined request system
  - Requests will be very diverse
  - Speed, speed, speed

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Standard OPS Dashboard - Windows

Deployed into the Password Manager Application



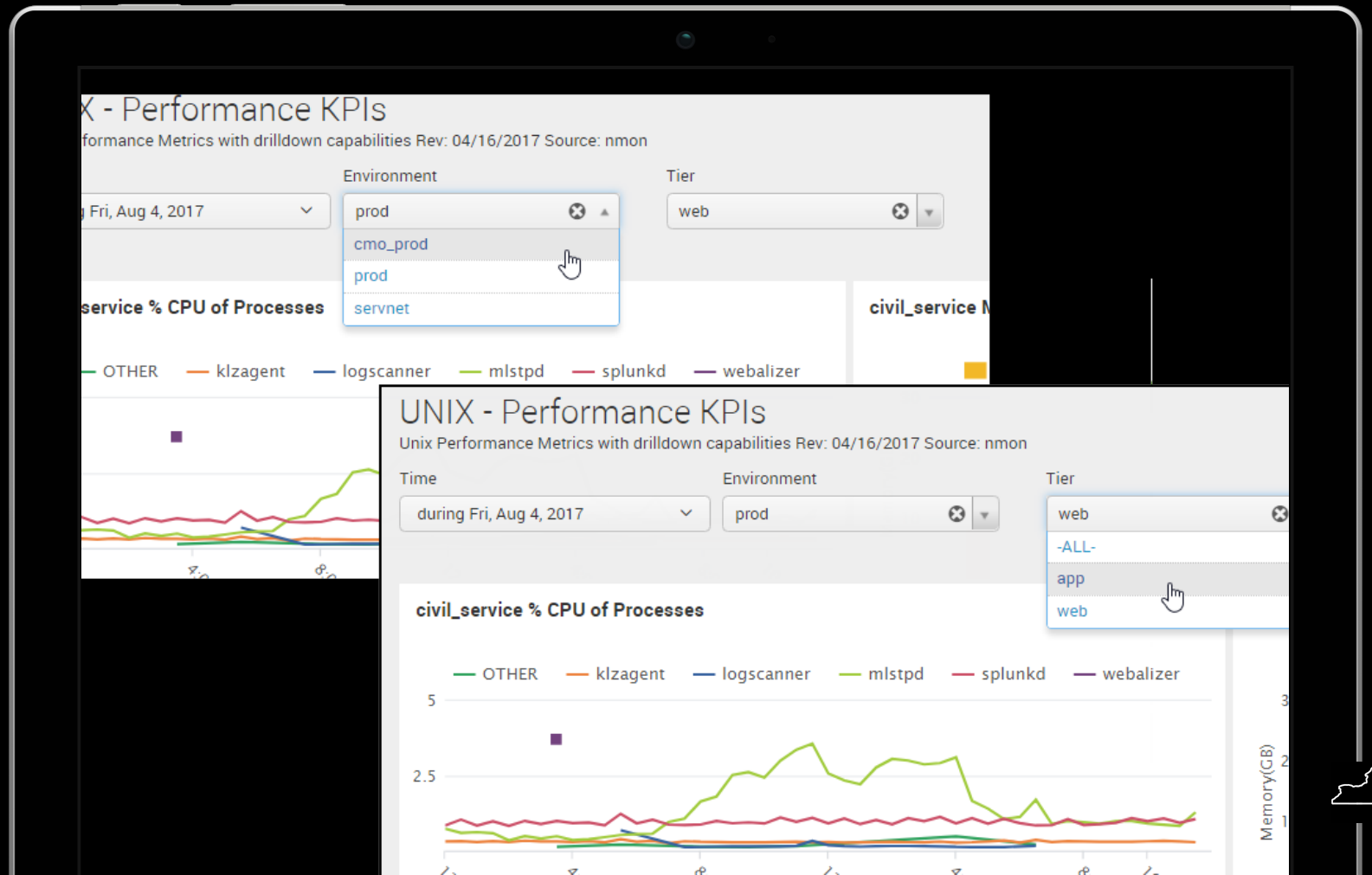
- Performance KPIs
  - Processor Time
  - Bandwidth Utilization
  - Page Faults
  - Disk Free

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Standard OPS Dashboard - UNIX

Deployed into the Password Manager Application



- Select Collection of Hosts by Function
  - Time
  - Environment
    - Prod, QA etc
  - Tier
    - Db, Web, App

The Use Case (civil service) is sensed automatically by being in the APP

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

How?

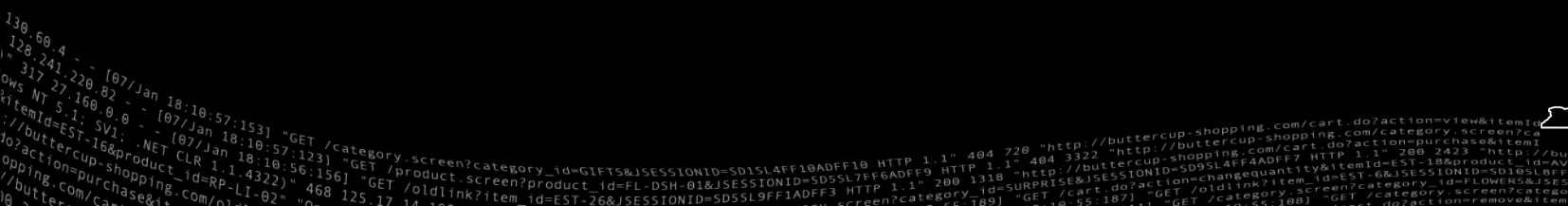
Make OPS dashboards auto sensing

1. ONBOARD lookup that organizes the hosts the way the user wants to see them.
2. SPLUNK_APPS lookup that ties the current APP name to the hosts needed.
3. Auto-sensing javascript in dashboards that knows the current APP.

Splunk Service Request

ITSM Service Request – Open to All

- Details about hosts, sources and sourcetypes
- Categorize hosts by:
  - Environment
  - Middleware Tier
- Business case justifying resources
  - Security requirements
  - Retention
  - Estimate of size
- Accept responsibility to inform Splunk Team of changes



NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Use Case Hierarchy

The hosts can be grouped into three levels

Tier 1

Application – Use Case – Splunk APP

Like Motor Voter, Pub1075, Excelsior, Biztalk, Aspera, DNS, Tivoli …

Tier 2

Environment – Stage of Development

Like Prod, Dev, Staging, Test, QA …

Tier 3

Tier – Software Classification

Like DB, Web, WAS, app … Multiply connected.

1. Onboard Lookup

Knowledge Object with Application Hierarchy

agency	use_case	environment	tier	host	ip
Dot	PRIMAVERA	Dev	Web	Host1	10.1.0.1
Dot	PRIMAVERA	Dev	Services	Host2	10.1.0.2
Dot	PRIMAVERA	Prod	Web	Host3	10.1.2.3
Dot	PRIMAVERA	Prod	Web	Host4	10.1.2.1
Dot	PRIMAVERA	Prod	Services	Host5	10.1.2.2

ONBOARD

Implemented by a Global Lookup

- Lookup Advantages over Tag
  - Global Knowledge Object
  - Easy to setup, change, test and deploy
  - Uses database tools to manage changes

Lookup table can be used to setup a search to find which hosts are *not* reporting data

2. SPLUNK_APPS Lookup

Zips the local APP name to Use Case

Local App Name	use_case
Justice_center	JUSTICE
Primavera	PRIMAVERA
Hesc	EXCELSIOR
Hunt_fish_ny	HUNTFISH
Biztalk	BIZTALK

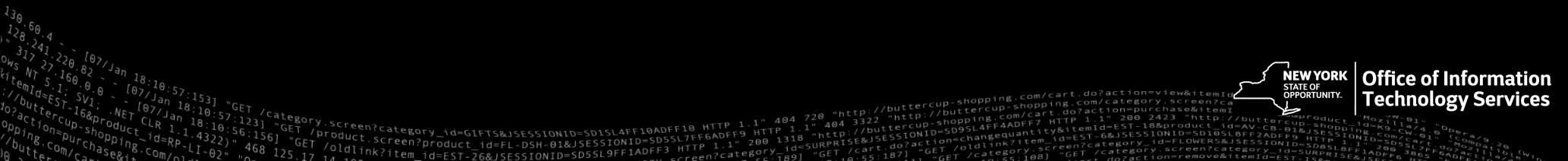
3. Autosense APP Name

Implemented by JavaScript

- To sense the current APP name, insert reference in the first line of the simple XML

```
<form script="set_app_token.js"> …
```

  - Creates app token
  - See Define Custom Tokens in Splunk 6.x Dashboard Examples
  - Built into Splunk 6.6



Self Adapting Dashboard Implemention

Use the 3 Knowledge Objects in the Simple XML

- Sense current, get APP name

```
<form
script="set_app_token.js"
> …
```

  - Creates app token
  - See Define Custom Tokens in Splunk 6.x Dashboard Examples
  - Built into Splunk 6.6

- Build Dropdowns from Lookups

```
<query>
| inputlookup onboard
| search
`use_case($app$)`
| fields stage
</query>
```

Incorporate into Panel query

```
<query> ..
[ | inputlookup onboard
| search
`use_case($app$)`
stage="$environment$"
tier=$tier$
| fields host ]
… </query>
```

So How Is It Fast and Easy?

We make the dashboard into a template!

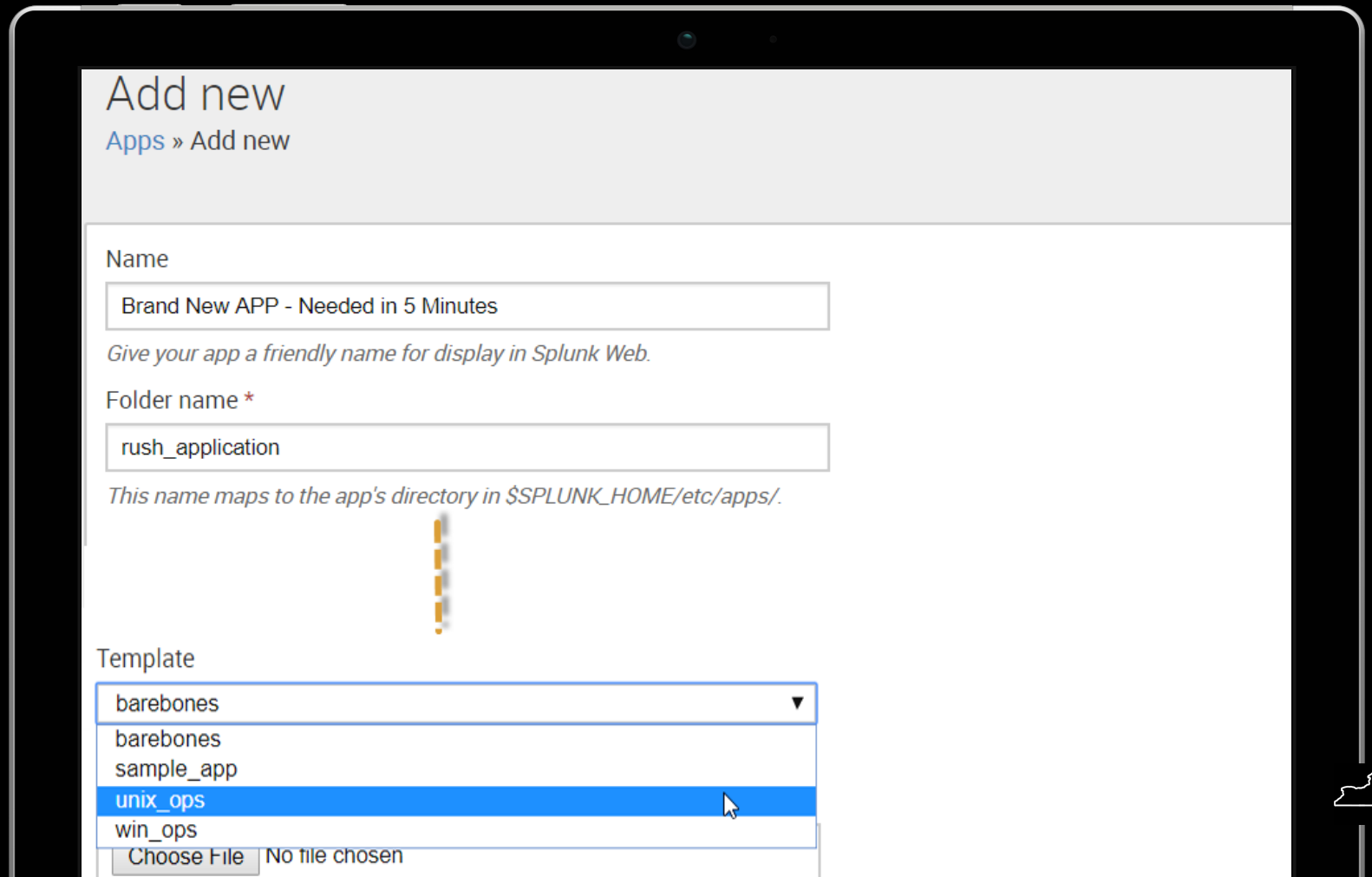
NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk>

.conf2017

New APP Creation

Standard OPS Dashboard Deployed Immediately



- Provisos:
  - ONBOARD Loaded
    - use_case
    - environment
    - tier
    - hosts
  - SPLUNK_APP Loaded
    - splunk_app
    - use_case

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Use Template for Rapid Deployment

Loads the OPS Dashboards on APP Creation

```
09:23:35 /splunk/splunk/share/splunk/app_templates
$ tree unix_ops
unix_ops
├── bin
│   └── README
├── default
│   ├── app.conf
│   └── data
│       └── ui
│           ├── nav
│           │   └── default.xml
│           └── views
│               ├── analysis_of_cpu_usage.xml
│               ├── analysis_of_network_rw_speed.xml
│               ├── …
└── metadata
    └── default.meta
```

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Results

Deploying Standard OPS Dashboards

- Value created as soon as the data arrives.
- Users do not have to create the standard dashboards.
- OPS dashboards are same across all applications for consistent comparison.
- Dashboard creation is automated. Fewer errors and more time for new features.

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

Splunk Team New York State

Office of Information Technology Systems
Barry Krawchuk, Research Scientist
Contact: barry.krawchuk@its.ny.gov
@thebarryk

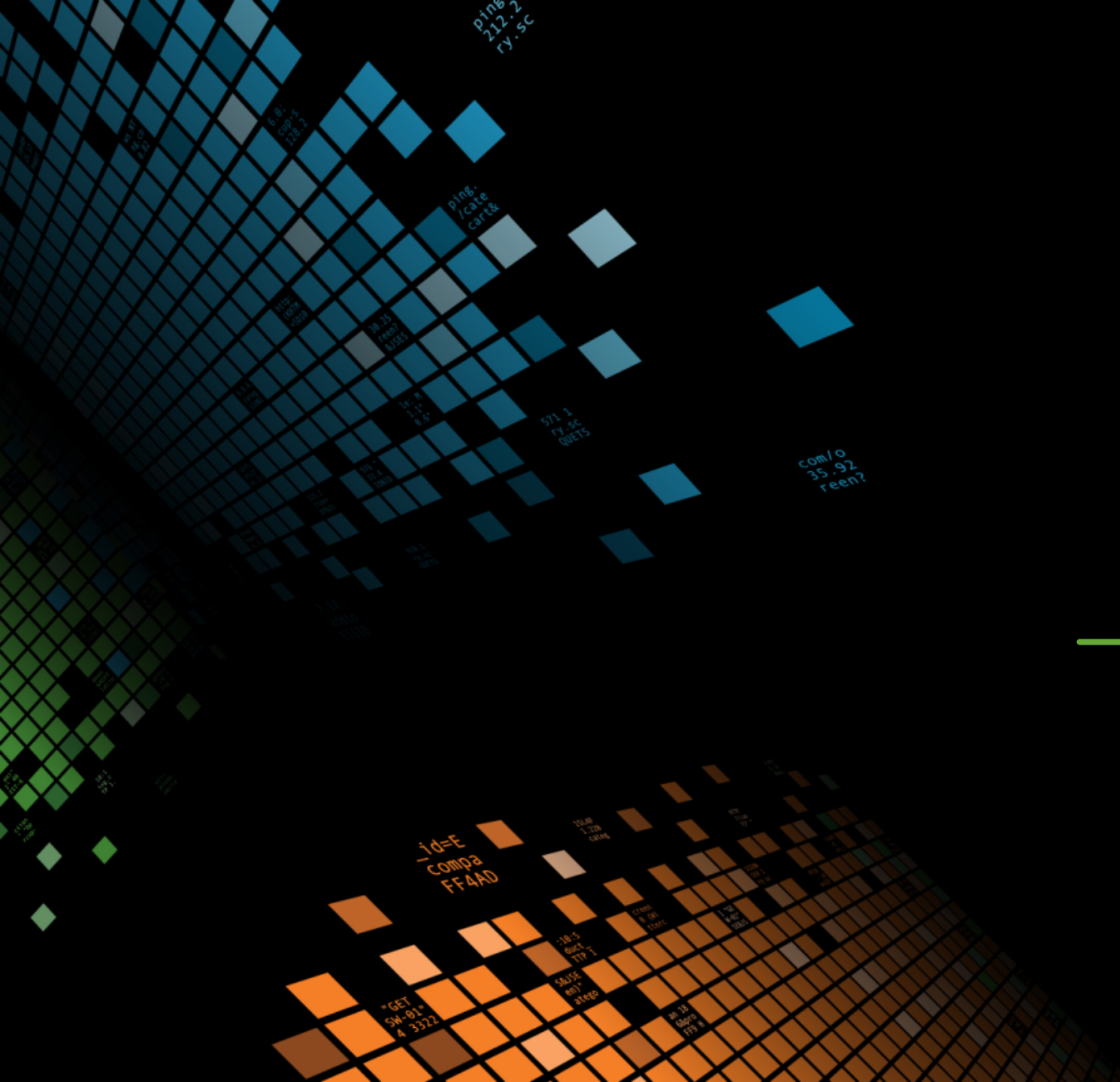
NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017

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

splunk> .conf2017

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services



APPENDIX

Some additional details

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk>

.conf2017

Acknowledgements

Splunk Team

- Admins: Jason Mantor and Ulrike Pohlig
- Developers: Jeff Irving, Bruce Shattuck
- Onboarding: Susan Brownell
- Network Developer: Craig Stillwell
- Intern: Christopher Mitchell

Fill the Dropdowns

Use current app and lookups to populate the dropdown menus

```
<form script="set_app_token.js">
  <label>UNIX - Performance KPIs</label>
  <fieldset autoRun="false" submitButton="true">
    <!-- ... time_range dropdown -->
    <!-- ... $environment$ dropdown -->
    <input type="dropdown" searchWhenChanged="true" token="environment">
      <label>Environment</label>
      <search>
        <query>| inputlookup onboard | search `use_case($app$)` | fields
        stage</query>
      </search>
      <fieldForLabel>stage</fieldForLabel>
      <fieldForValue>stage</fieldForValue>
    </input>
    <!-- ... $tier$ dropdown -->
    <input type="dropdown" searchWhenChanged="true" token="tier">
      <label>Tier</label>
      <search>
        <query>| inputlookup splunk_onboard | search `use_case($splunk_app$)`
        stage="$environment$" | table tier | dedup tier | sort tier</query>
      </search>
      <fieldForLabel>tier</fieldForLabel>
      <fieldForValue>tier</fieldForValue>
    </input>
  </fieldset>
```

Build the Query

Use the dropdown tokens to complete the search

```
<row>
  <panel>
    <!-- % CPU of Processes -->
    <chart>
      <title>$app$ % CPU of Processes</title>
      <search>
        <query>
        index=nmon source=perfdata
        [ | inputlookup onboard
          | search `use_case($app$)`
            stage=$environment$ tier=$tier$
          | table host | dedup host ]
        Command!=watchdog/0
        | timechart limit=5 avg(pct_CPU) as pct_CPU by Command
        </query>
        <earliest>$time_range.earliest$</earliest>
        <latest>$time_range.latest$</latest>
      </search>
    </chart>
  </panel>
</row>
</form>
```

Template Guidelines

Hints

- Include all the children drilldown dashboards
  - If a Library app is used the user gets confused when the app context changes
- Make children dashboards invisible unless they can standalone. Prevent user from clicking it in dashboard list.
  - <form isVisible="false">
- Protect all the dashboards from change in default.meta
  - access = read : [*], write : [admin]

Modification of Standard OPS

Use Deployment Server

- Create serverclass for each set standard dashboards
  - serverClass:searchhead_std_apps
  - Populate with searchhead to receive standard dashboard
- Create serverclass app for each installed app
  - app:aspera
  - Etc …
- On deployment server in ..deployment-apps/
  - Create folder aspera
  - cp -r of production folder unix_ops (softlink?)

Future

Additional OPS Dashboards

- Server load, database connects
- SCOM and/or Tivoli Alerts
- ITSM changes/ incidents/ request
- IPS Warnings and Threats
- Certificate status
- CIM compliance
- KPI collection for ITSI glass tables
- Standard dashboards for Web Servers

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

splunk> .conf2017