splunk> .conf2017

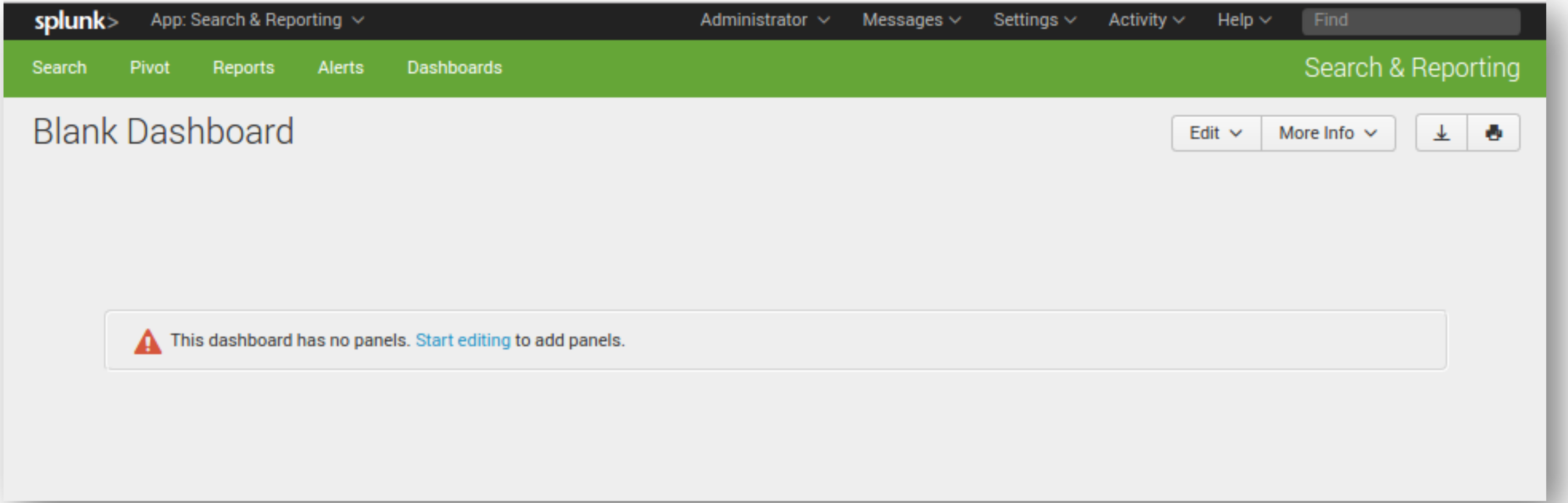
Tokens In Splunk Web Framework

Use, Abuse, And Incantations

Ryan Thibodeaux | VP of Operations, OctoInsight Inc.

September 26th, 2017 | Washington, DC

How Many Tokens Are In This Dashboard?



Blank Dashboard

This dashboard has no panels. Start editing to add panels.

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.

Who Is This Guy?

- VP of Operations / Splunk Dev at OctoInsight Inc.
- Splunk app developer since 2014 (Layer8* App for Splunk)
- SplunkTrust Community MVP 2016 – 2018
- Co-organizer of WashDC Splunk User Group

SPLUNK TRUST

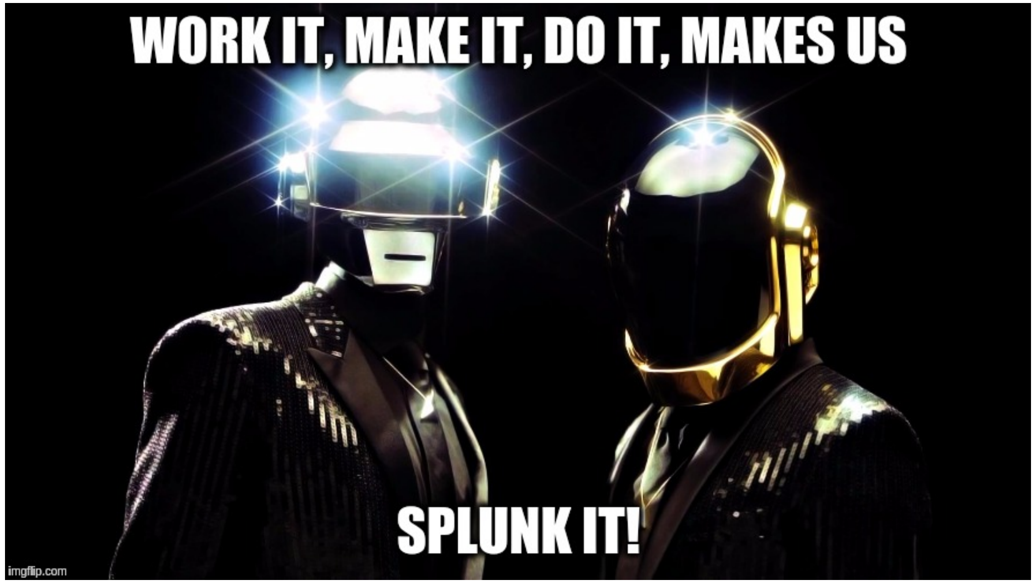
- Splunk blog: https://blog.octoinsight.com/tag/splunk
- Splunk Answers: @rjthibod
- Splunk Slack: @artie73

splunk> .conf2017

Session Goals & Agenda

Making you a superior Splunk Developer - i.e. Better, Faster, Stronger!

- Why do we care about tokens?
- Background
- Token debugging
- Compatibility and tokens
- Examples … becoming a to token ninja



Session Assumptions

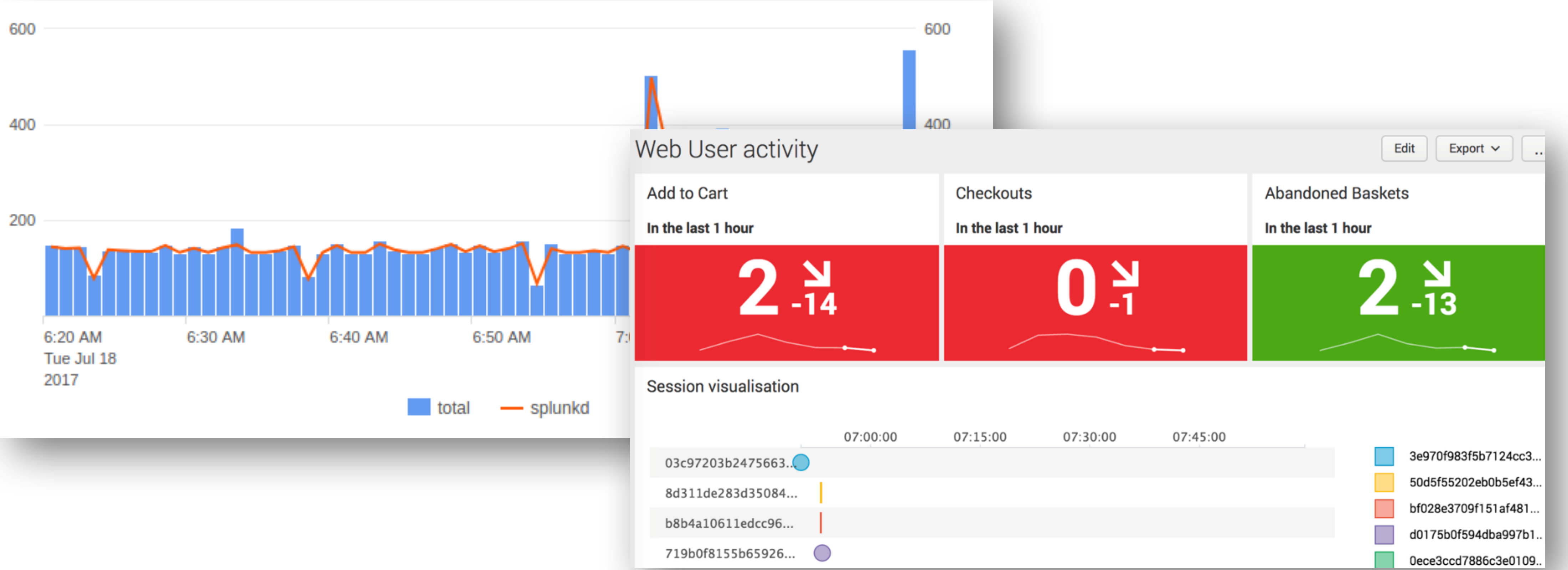
- Pre-reqs
  - Basic token syntax: `$TOKEN_NAME$, $form.TOKEN_NAME$`
  - Common token elements: `<change>, <condition>, <set>, <unset>`
  - Search event elements: `<done>, <progress>, <finalized>`
  - Form inputs and search elements in SimpleXML

- Resources
  - Docs - https://docs.splunk.com/Documentation/Splunk/latest/viz/tokens
  - .conf 2016 - Dashboard Wizardry: Advanced Dashboard Interactivity
  - .conf 2015 - Enhancing Dashboards with JavaScript!

Why Tokens Matter?

Where Tokens Matter Less

Are your dashboards simple?



Web User activity

Add to Cart

In the last 1 hour

2 -14

Checkouts

In the last 1 hour

0 -1

Abandoned Baskets

In the last 1 hour

2 -13

Session visualisation

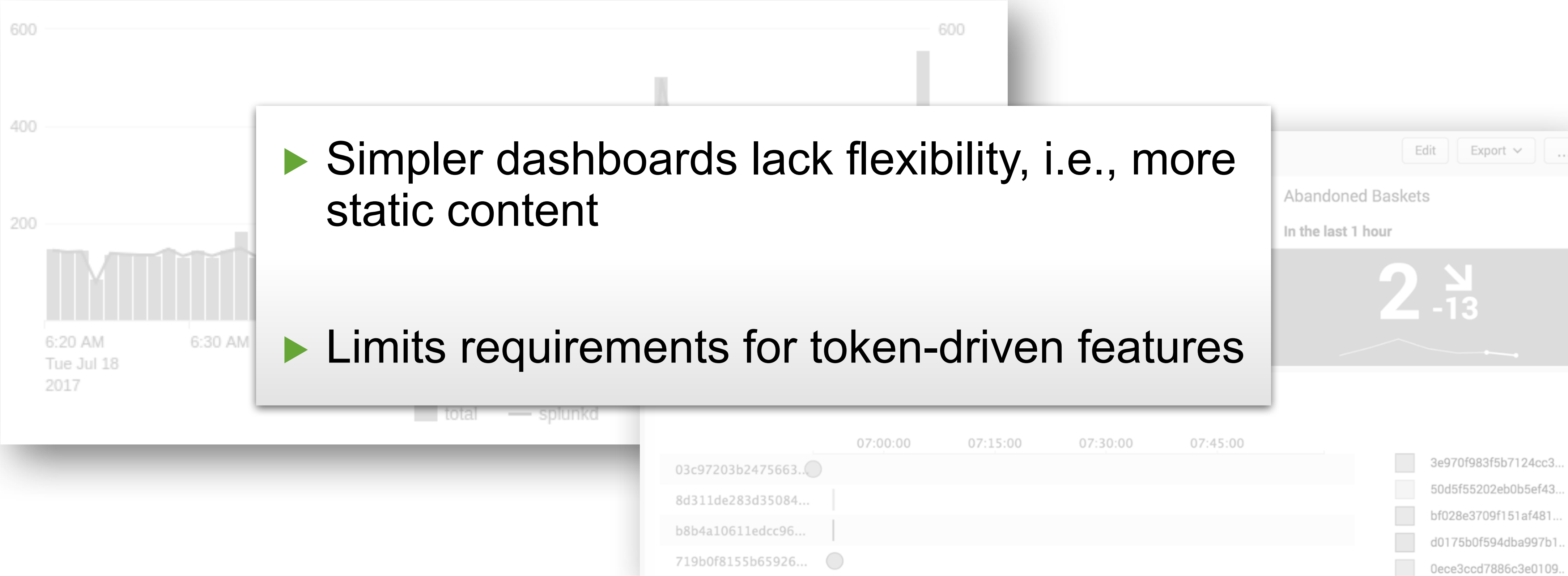
07:00:00 07:15:00 07:30:00 07:45:00

03c97203b2475663...
8d311de283d35084...
b8b4a10611edcc96...
719b0f8155b65926...

3e970f983f5b7124cc3...
50d5f55202eb0b5ef43...
bf028e3709f151af481...
d0175b0f594dba997b1...
0ece3ccd7886c3e0109...

Where Tokens Matter Less

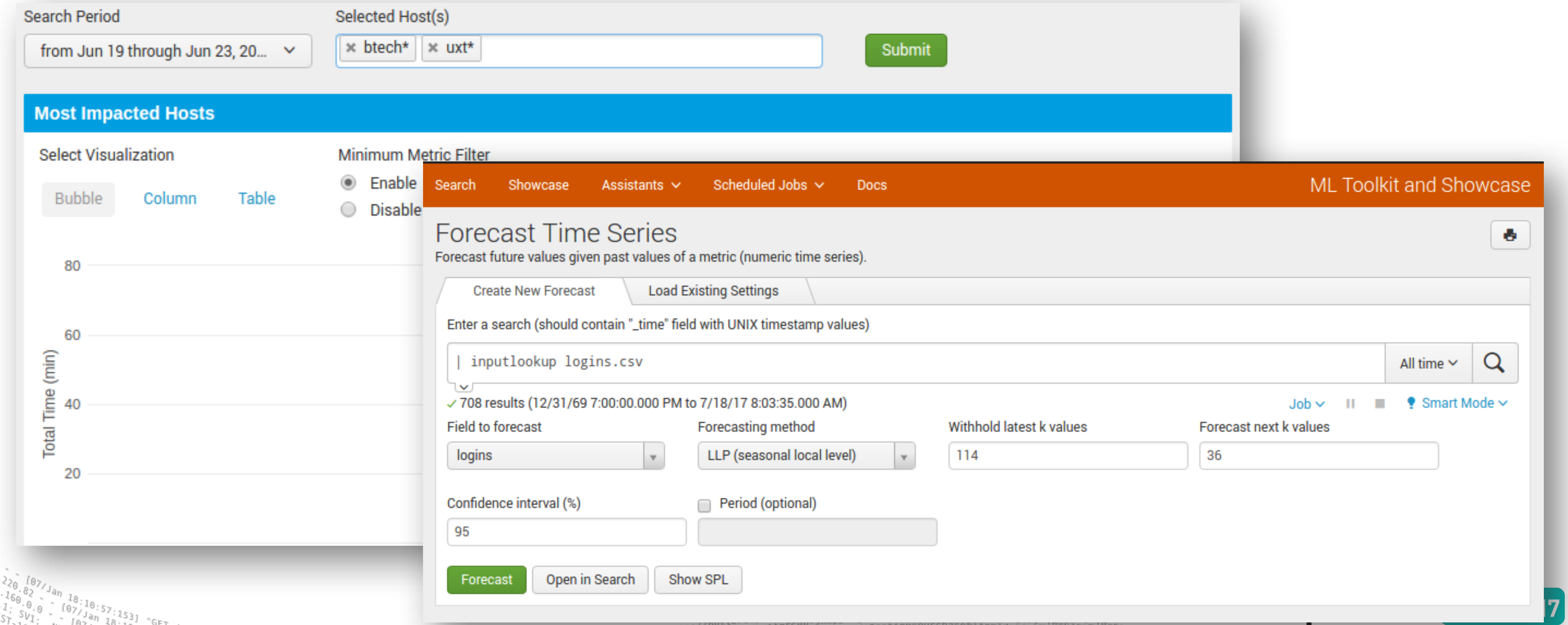
Are your dashboards simple?



- Simpler dashboards lack flexibility, i.e., more static content
- Limits requirements for token-driven features

Where Tokens Really Matter

Use cases demanding flexibility and complexity



Search Period: from Jun 19 through Jun 23, 20...

Selected Host(s): btech*, uxt*

Forecast Time Series

Forecast future values given past values of a metric (numeric time series).

Enter a search (should contain "_time" field with UNIX timestamp values)

```
| inputlookup logins.csv
```

All time

✓ 708 results (12/31/69 7:00:00.000 PM to 7/18/17 8:03:35.000 AM)

Field to forecast: logins

Forecasting method: LLP (seasonal local level)

Withhold latest k values: 114

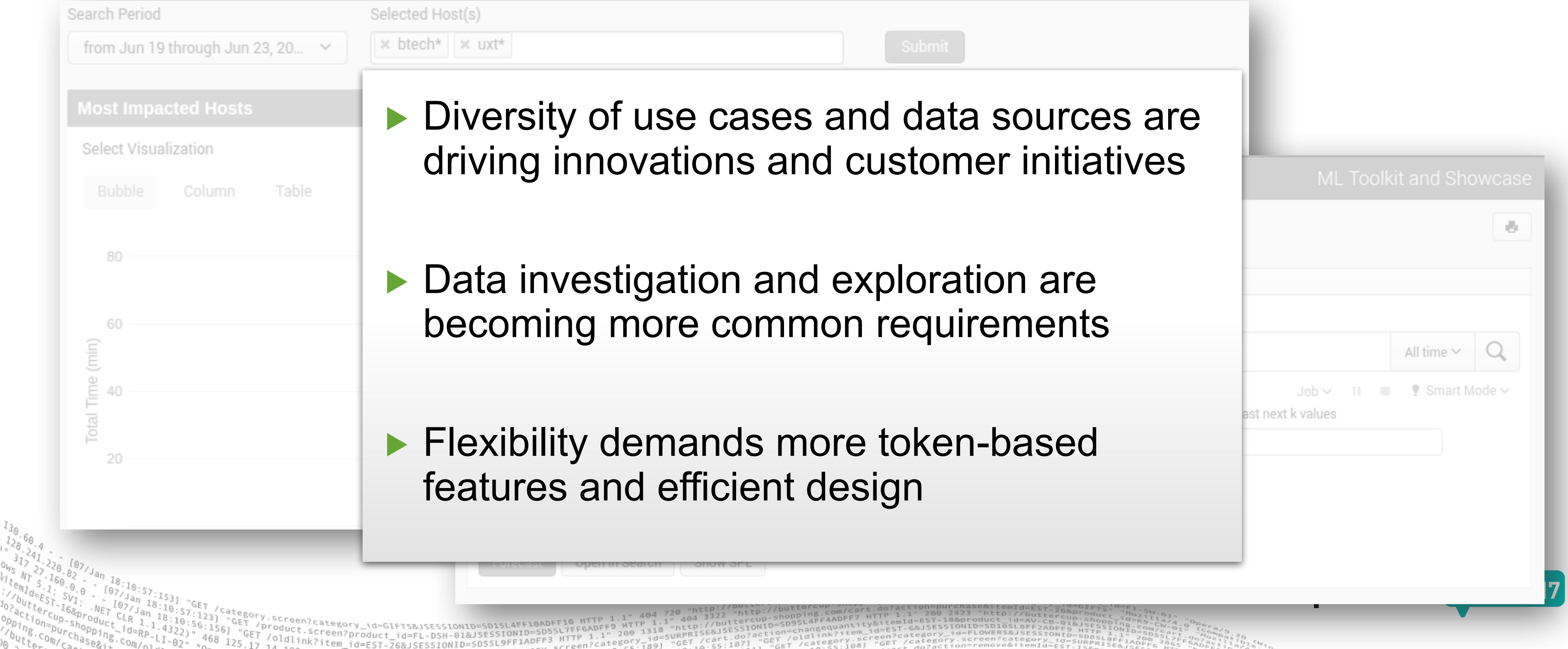
Forecast next k values: 36

Confidence interval (%): 95

□ Period (optional)

Where Tokens Really Matter

Use cases demanding flexibility and complexity

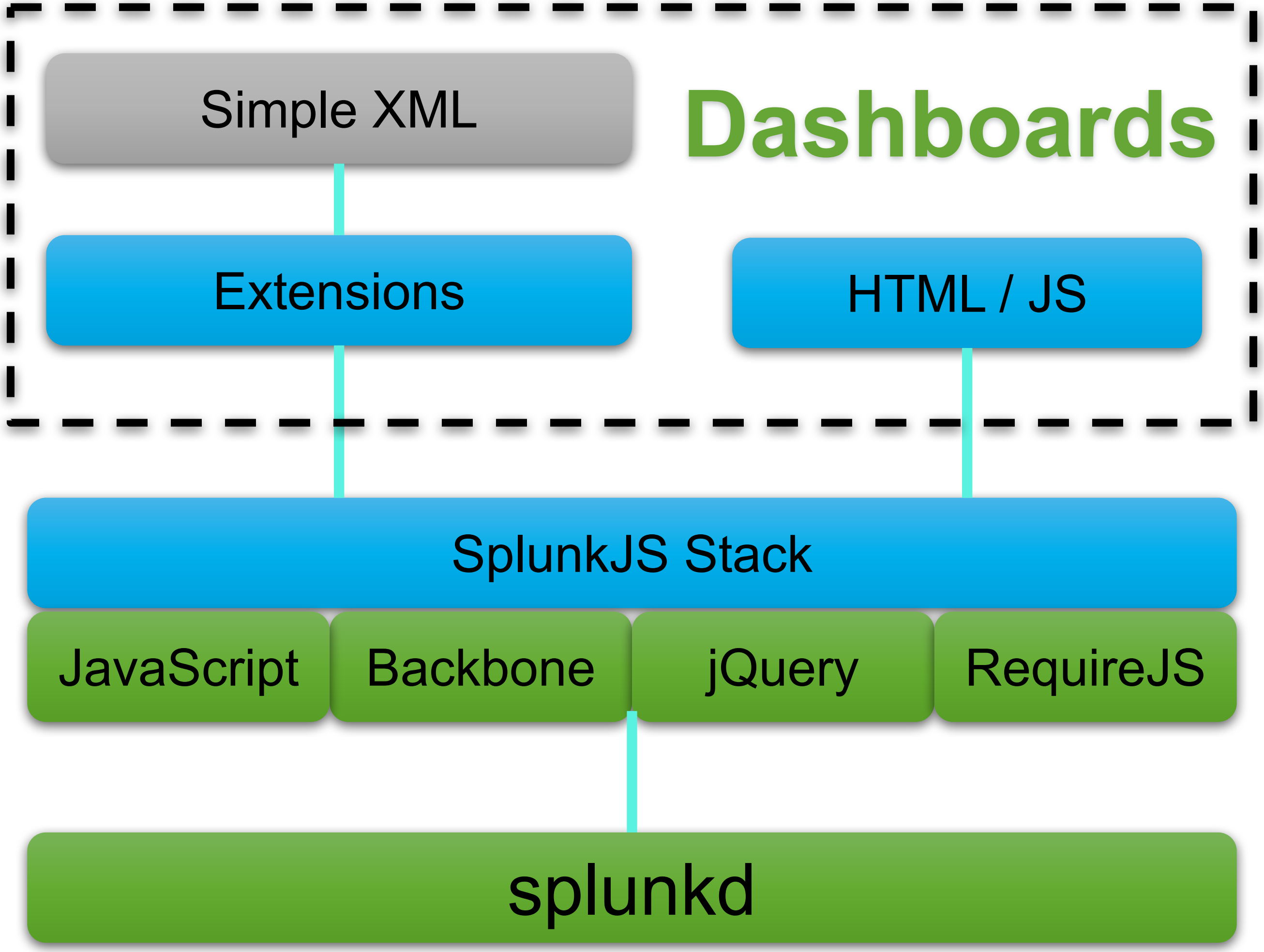


- Diversity of use cases and data sources are driving innovations and customer initiatives
- Data investigation and exploration are becoming more common requirements
- Flexibility demands more token-based features and efficient design

Tokens Background

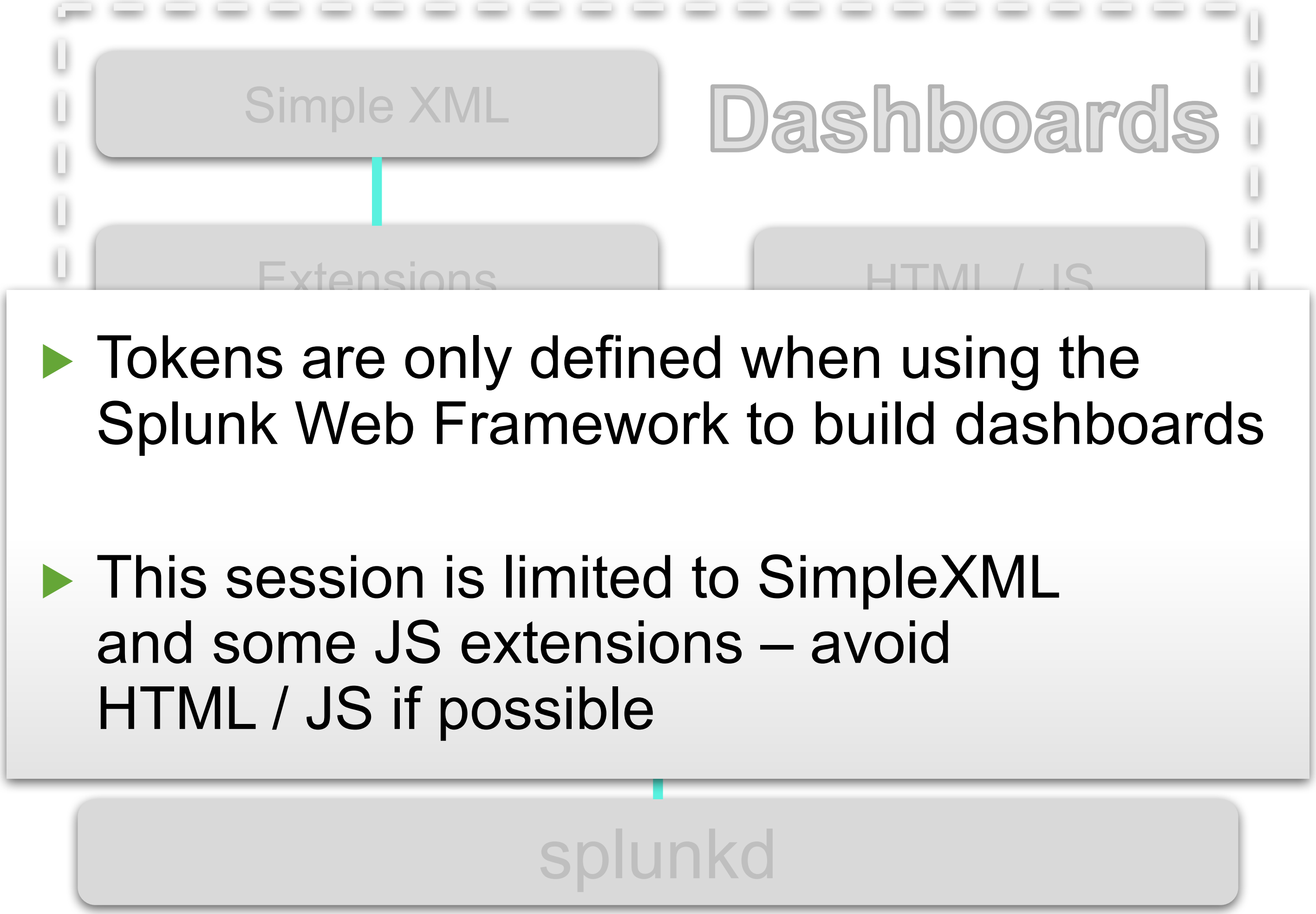
What Digging In The Docs Will Reveal

Splunk Web Stack And Dashboards



http://dev.splunk.com/webframework

Splunk Web Stack And Dashboards



- Tokens are only defined when using the Splunk Web Framework to build dashboards
- This session is limited to SimpleXML and some JS extensions – avoid HTML / JS if possible

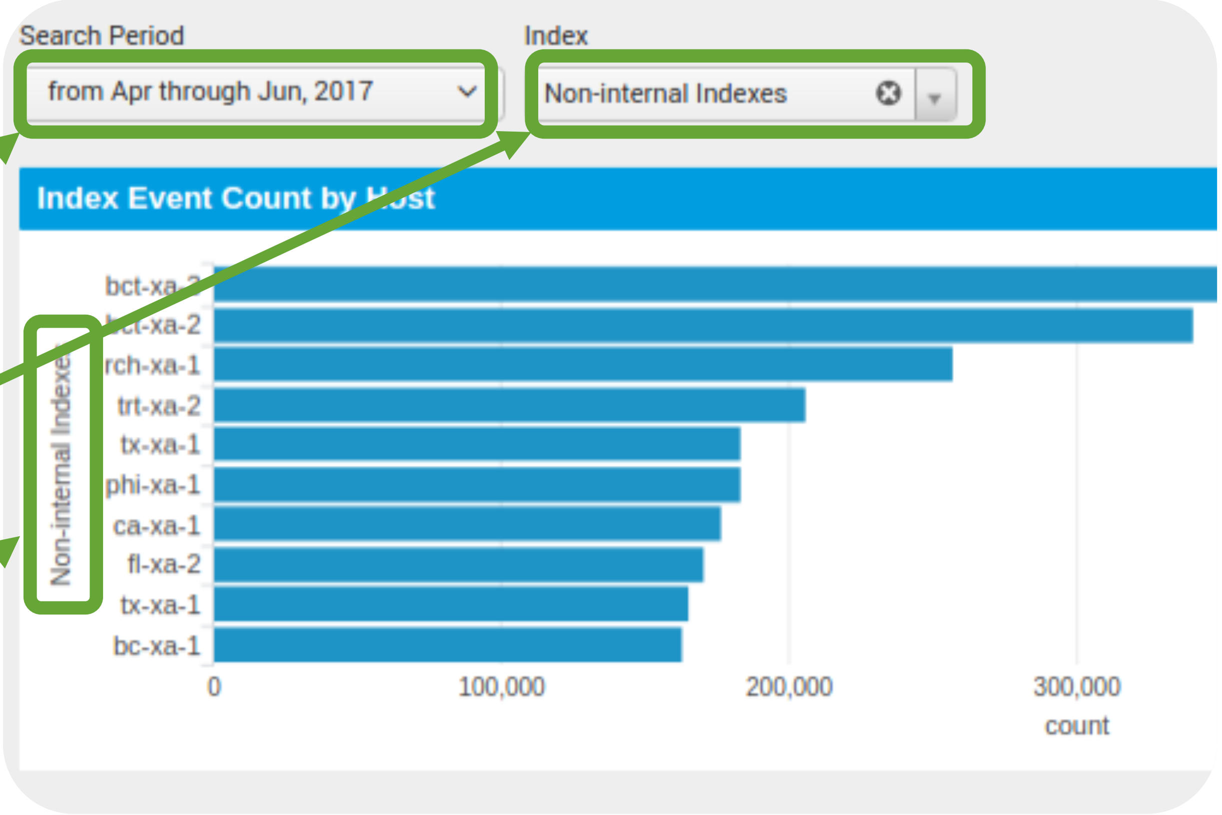
http://dev.splunk.com/webframework

splunk> .conf2017

Tokens In Dashboards

Maintain and transfer state

- Tokens ≈ Variables for SimpleXML
  - Reflect states in the dashboard
  - Can be user-driven, event-driven, or static
- Used to control and monitor searches and visualizations
  - Setting search time periods
  - User and Drilldown Inputs
  - Saving search results
  - Detecting search states / events
  - Adjusting Viz settings / output

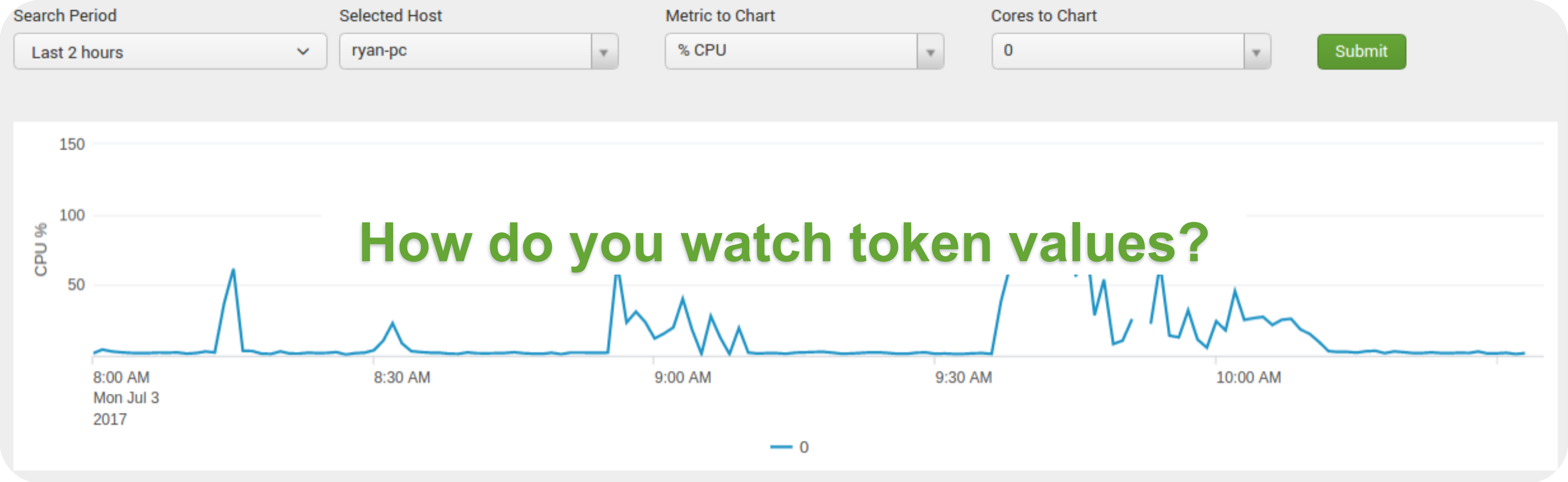


Search Period: from Apr through Jun, 2017

Index: Non-internal Indexes

Index Event Count by Host

Token Debugging



Search Period: Last 2 hours

Selected Host: ryan-pc

Metric to Chart: % CPU

Cores to Chart: 0

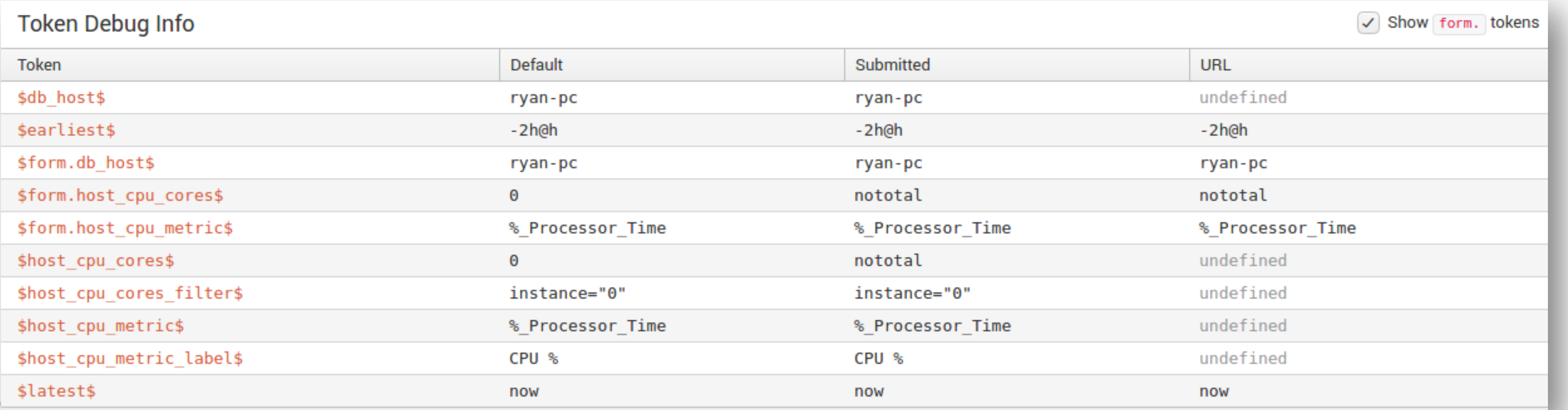
How do you watch token values?

Token Debugging

Watching token states

Splunk 6.x Dashboard Examples App includes showtokens.js

```
<form script="simple_xml_examples:showtokens.js">
```



Token Debug Info

☑ Show form. tokens

Token	Default	Submitted	URL
db_host	ryan-pc	ryan-pc	undefined
$earliest$	-2h@h	-2h@h	-2h@h
$form.db_host$	ryan-pc	ryan-pc	ryan-pc
$form.host_cpu_cores$	0	nototal	nototal
$form.host_cpu_metric$	%_Processor_Time	%_Processor_Time	%_Processor_Time
$host_cpu_cores$	0	nototal	undefined
$host_cpu_cores_filter$	instance="0"	instance="0"	undefined
$host_cpu_metric$	%_Processor_Time	%_Processor_Time	undefined
$host_cpu_metric_label$	CPU %	CPU %	undefined
$latest$	now	now	now

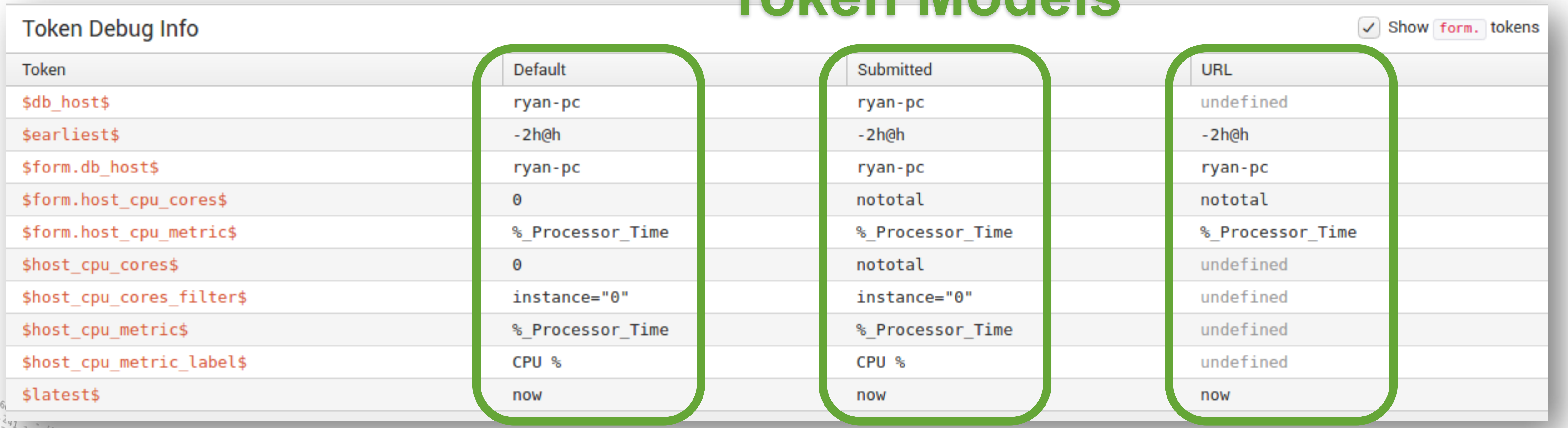
Token Debugging

Watching token states

Splunk 6.x Dashboard Examples App includes showtokens.js

```
<form script="simple_xml_examples:showtokens.js">
```

Token Models



Token Debug Info

✓ Show form. tokens

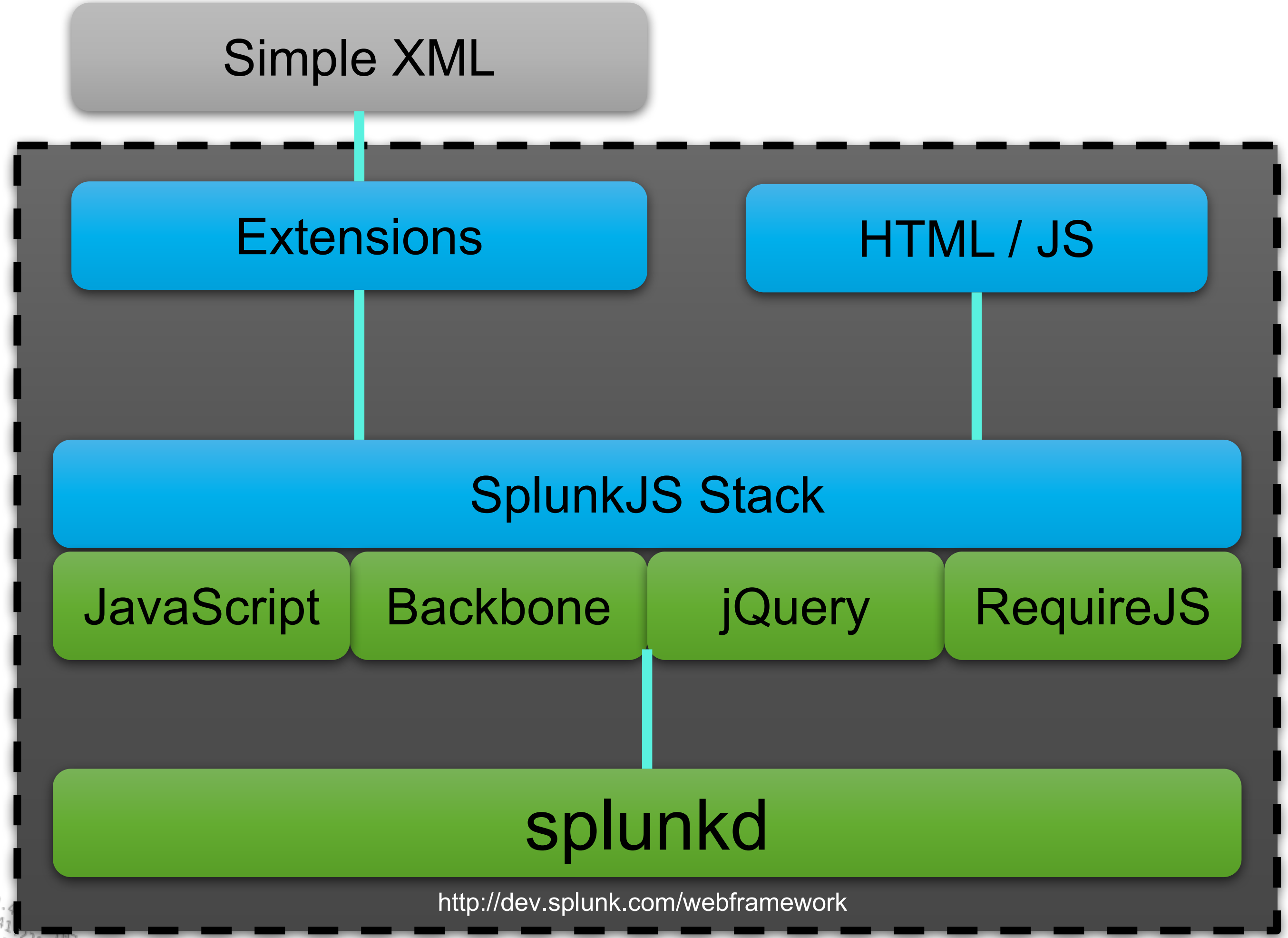
Token	Default	Submitted	URL
db_host	ryan-pc	ryan-pc	undefined
$earliest$	-2h@h	-2h@h	-2h@h
$form.db_host$	ryan-pc	ryan-pc	ryan-pc
$form.host_cpu_cores$	0	nototal	nototal
$form.host_cpu_metric$	%_Processor_Time	%_Processor_Time	%_Processor_Time
$host_cpu_cores$	0	nototal	undefined
$host_cpu_cores_filter$	instance="0"	instance="0"	undefined
$host_cpu_metric$	%_Processor_Time	%_Processor_Time	undefined
$host_cpu_metric_label$	CPU %	CPU %	undefined
$latest$	now	now	now

Tokens And Compatibility

New Features, New Problems

Splunk Web Stack And Features

Dashboard compatibility and development



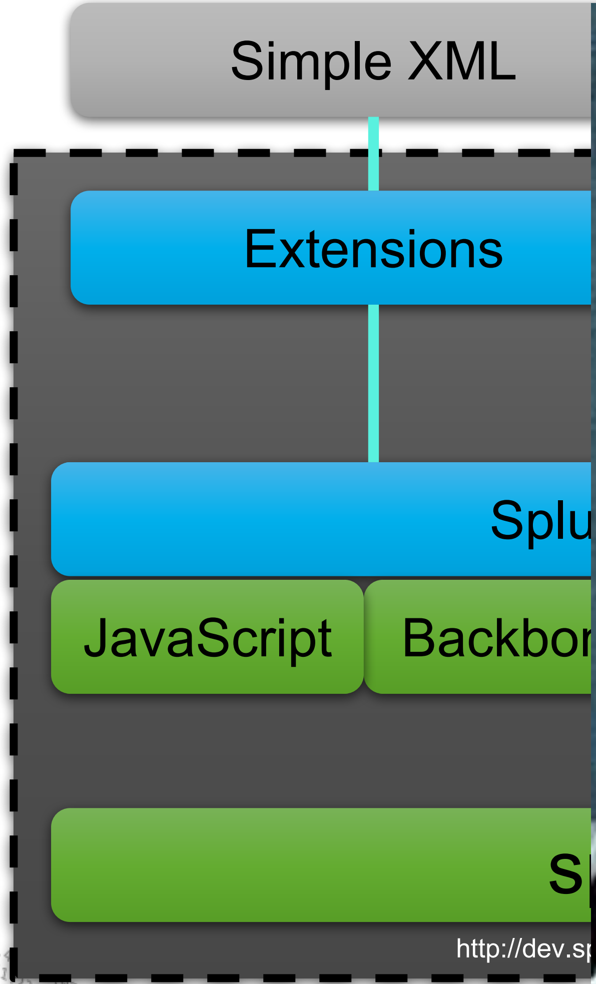
http://dev.splunk.com/webframework

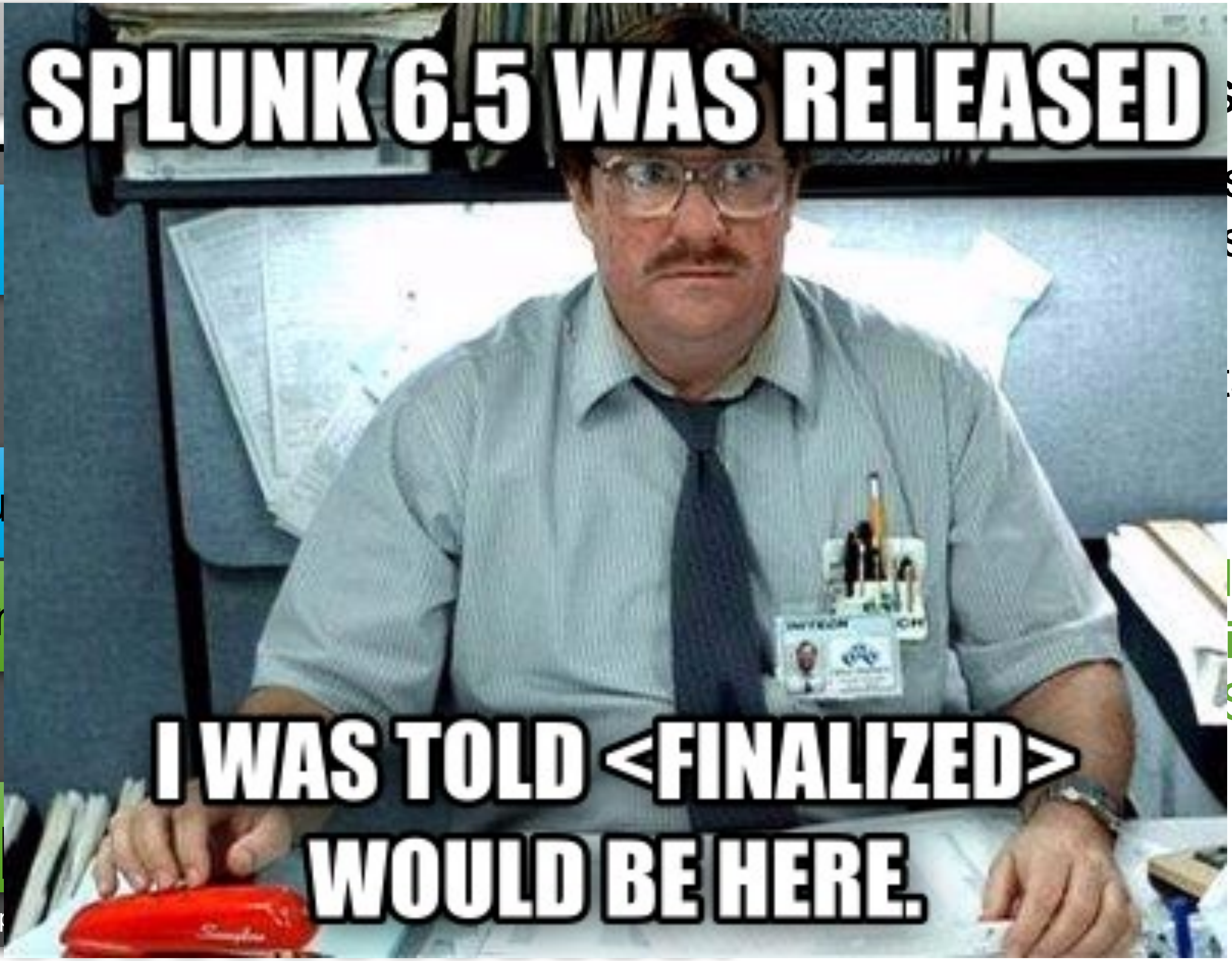
- SimpleXML vs. Everything Else
  - SimpleXML has added many token-related features since Splunk 6.2
  - The remaining components remain relatively constant in terms of tokens and events

Developers must decide on the required feature set. Sometimes implementing something in JavaScript is required for compatibility sake.

Splunk Web Stack And Features

Dashboard compatibility and development





. Everything Else

s added many token-
s since Splunk 6.2

components remain
ant in terms of tokens

lecide on the required
imes implementing
Script is required for

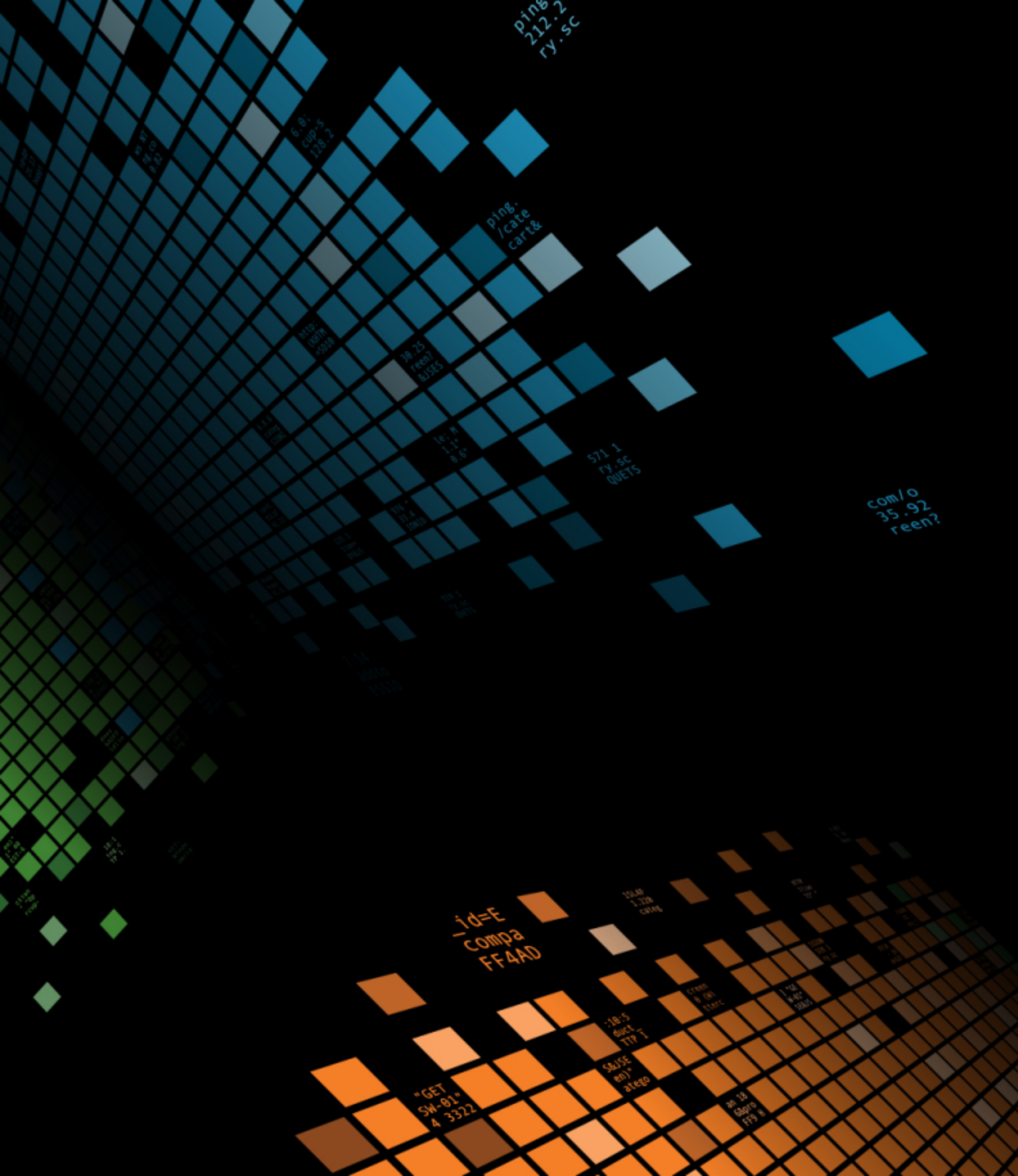
Ch-ch-ch-ch-Changes In `<change>`

Be aware of subtle token syntax differences

- In Splunk < 6.3
  - Always use `$token$` format, but it only applies to `<set>` and `<unset>`
  - No tokens allowed in `<condition>`
  - No support for `<eval>`

- In Splunk 6.3 & 6.4
  - Use `$token$` format in `<set>` and `<unset>`
  - Use single quote `'token'` format in `<condition>` and `<eval>`

- In Splunk >= 6.5
  - Can use `$token$` format everywhere if you don't support older versions
  - Still use single quote `'token'` format in `<condition>` and `<eval>` to maintain backwards compatibility



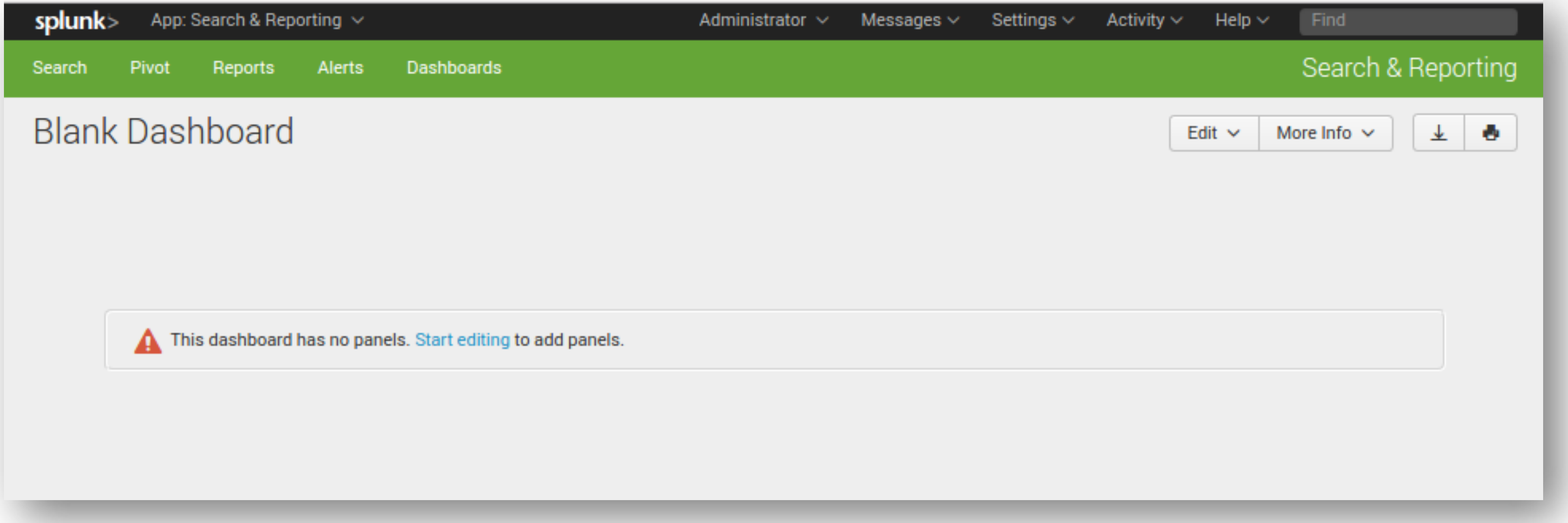
Tokens In Action

What You Find Out From Experience

Tokens in Dashboards

They are ever present

How many tokens are in this dashboard?

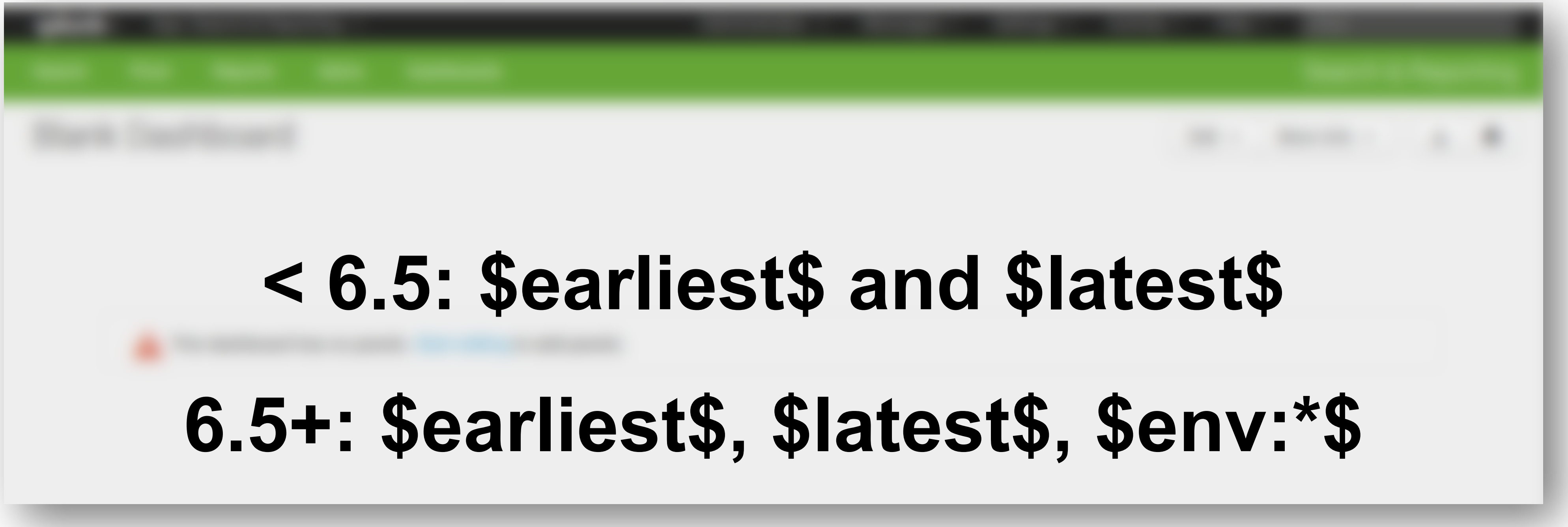


This dashboard has no panels. Start editing to add panels.

Tokens in Dashboards

They are ever present

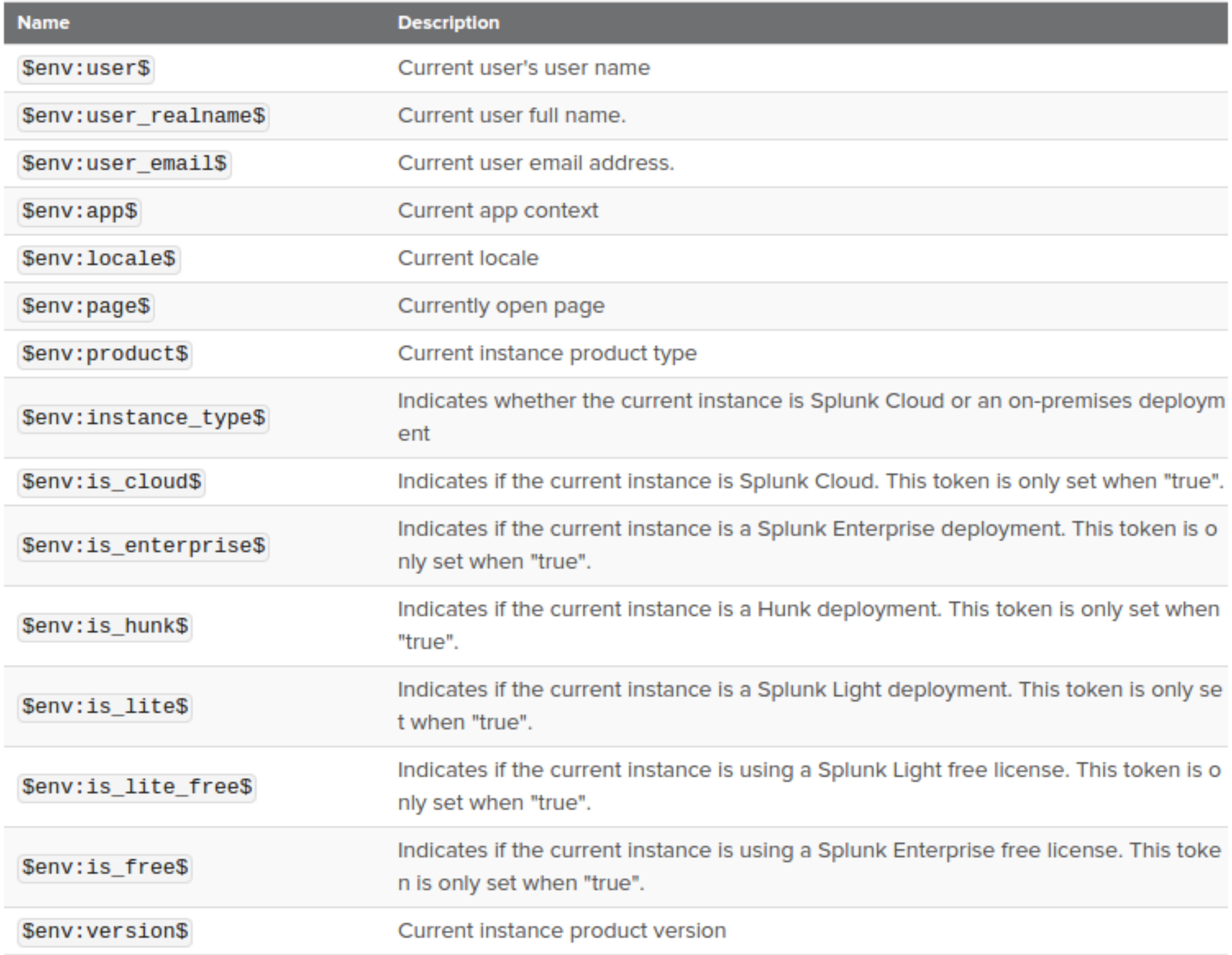
How many tokens are in this dashboard?



< 6.5: $earliest$ and $latest$

6.5+: $earliest$, $latest$, $env:*$

https://docs.splunk.com/Documentation/Splunk/latest/Viz/tokens #Use_global_tokens_to_access_environment_information



Name	Description
`$env:user$`	Current user's user name
`$env:user_realname$`	Current user full name.
`$env:user_email$`	Current user email address.
`$env:app$`	Current app context
`$env:locale$`	Current locale
`$env:page$`	Currently open page
`$env:product$`	Current instance product type
`$env:instance_type$`	Indicates whether the current instance is Splunk Cloud or an on-premises deployment
`$env:is_cloud$`	Indicates if the current instance is Splunk Cloud. This token is only set when "true".
`$env:is_enterprise$`	Indicates if the current instance is a Splunk Enterprise deployment. This token is only set when "true".
`$env:is_hunk$`	Indicates if the current instance is a Hunk deployment. This token is only set when "true".
`$env:is_lite$`	Indicates if the current instance is a Splunk Light deployment. This token is only set when "true".
`$env:is_lite_free$`	Indicates if the current instance is using a Splunk Light free license. This token is only set when "true".
`$env:is_free$`	Indicates if the current instance is using a Splunk Enterprise free license. This token is only set when "true".
`$env:version$`	Current instance product version

Time Tokens in Dashboards

Be careful with global time picker tokens

If you use a **custom token name** for your **time picker**, the **global time tokens $earliest$** and **$latest$** are still defined for **“All Time”**

```
<search>
  <query>
    index=… earliest=$dbtime.earliest$ latest=$dbtime.latest$
    | …
    | append [ search index=… |  … ]
  </query>
</search>
```

Time Tokens in Dashboards

Be careful with global time picker tokens

If you use a **custom token name** for your **time picker**, the **global time tokens $earliest$** and **$latest$** are still defined for **“All Time”**

```
<search>
  <query>
    index=… earliest=$dbtime.earliest$ latest=$dbtime.latest$
    | …
    | append [ search index=… |  … ]
  </query>
</search>
```

splunk> .conf2017

Time Tokens in Dashboards

Be careful with global time picker tokens

If you use a **custom token name** for your **time picker**, the **global time tokens $earliest$** and **$latest$** are still defined for **“All Time”**

```
<search>
  <query>
    index=…
    | …
    | append [ search index=… |  … ]
  </query>
  <earliest>$dbtime.earliest$</earliest>
  <latest>$dbtime.latest$</latest>
</search>
```

Always safer

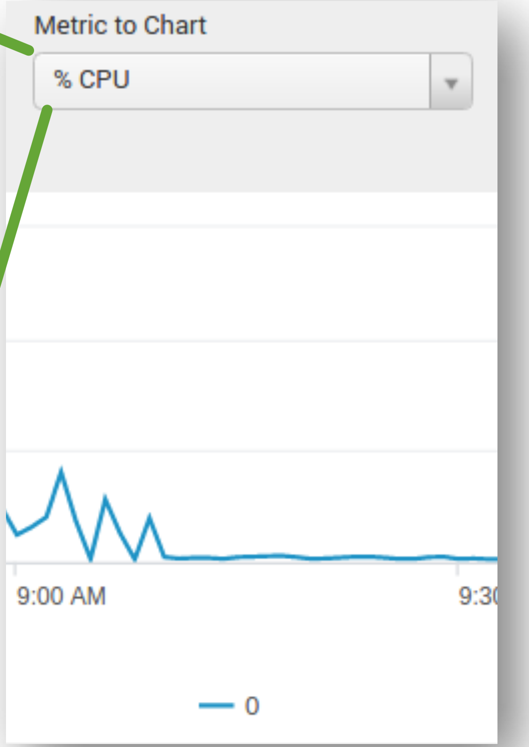
Demo: Input Tokens

Input Tokens

Second-level tokens do not behave the same

As of Splunk 6.6, **searchWhenChanged** does **not impact** tokens in **<change>**

```
<input searchWhenChanged="false" token="host_cpu_metric" …>
  <label>Metric to Chart</label>
    …
  <change>
    <condition label="PQL">
      <set token="form.host_cpu_cores">all</set>
      <set token="host_cpu_metric_label">PQL Count</set>
    </condition>
    <condition value="*">
      <set token="host_cpu_metric_label">CPU %</set>
    </condition>
  </change>
  …
```



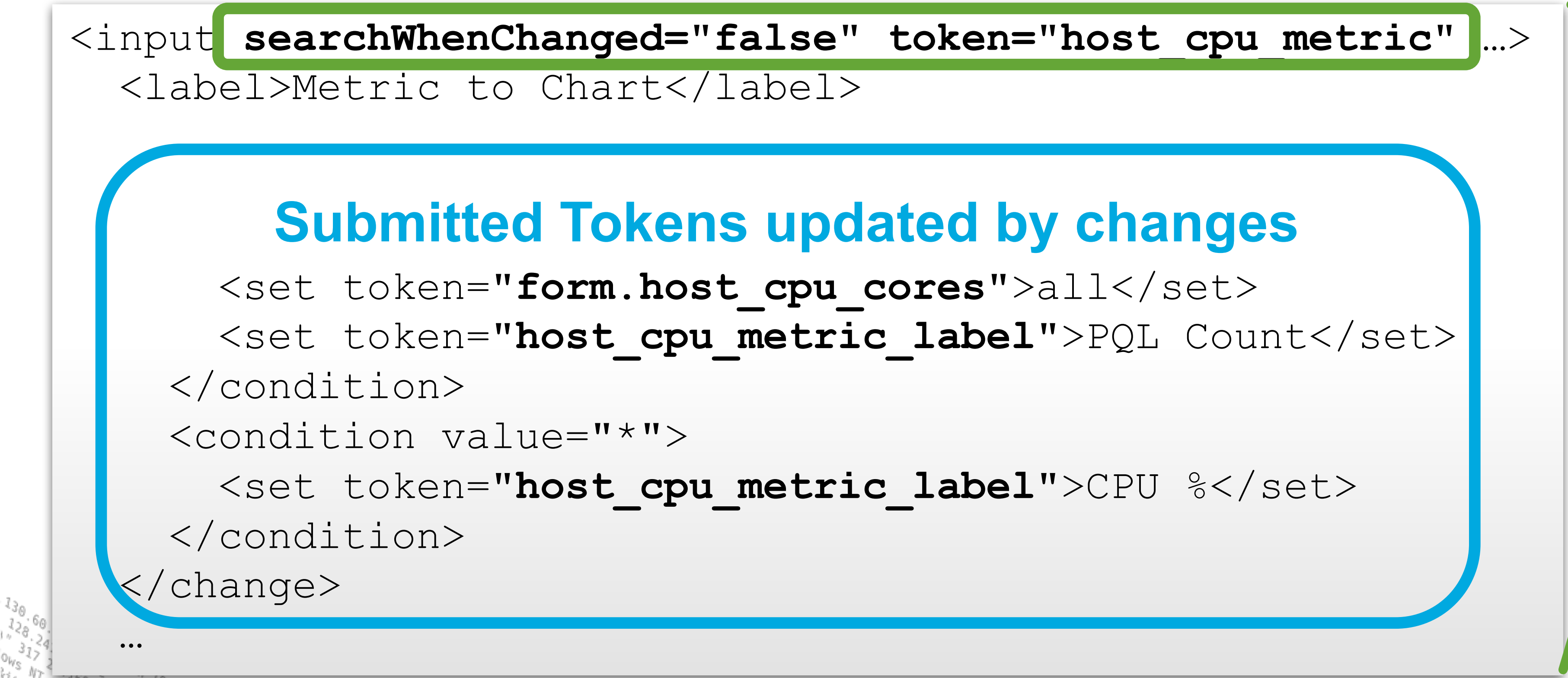
Metric to Chart: % CPU

Input Tokens

Second-level tokens do not behave the same

As of Splunk 6.6, **searchWhenChanged** does **not impact** tokens in **<change>**

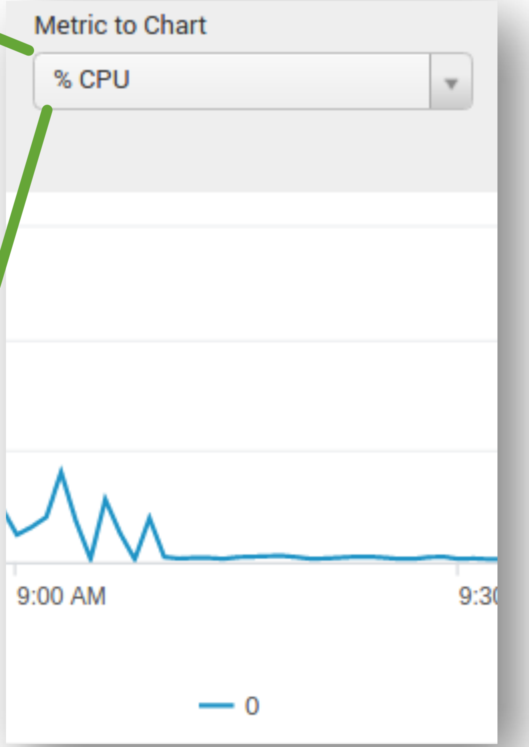
Only Default Token updates with change



```
<input searchWhenChanged="false" token="host_cpu_metric" …>
  <label>Metric to Chart</label>
```

Submitted Tokens updated by changes

```
      <set token="form.host_cpu_cores">all</set>
      <set token="host_cpu_metric_label">PQL Count</set>
    </condition>
    <condition value="*">
      <set token="host_cpu_metric_label">CPU %</set>
    </condition>
  </change>
  …
```



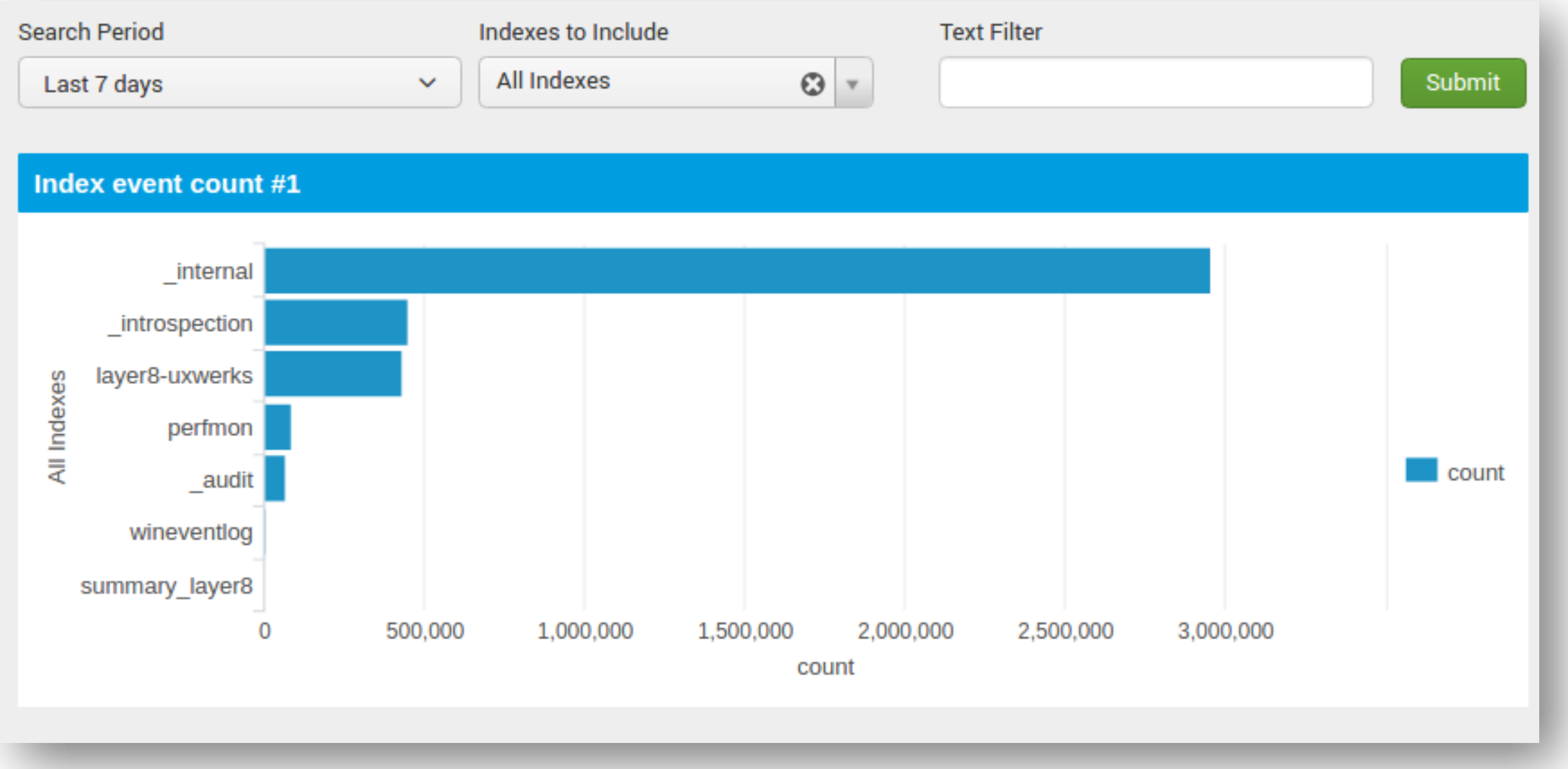
Metric to Chart

% CPU

Text Input Tokens

Empty values are not undefined

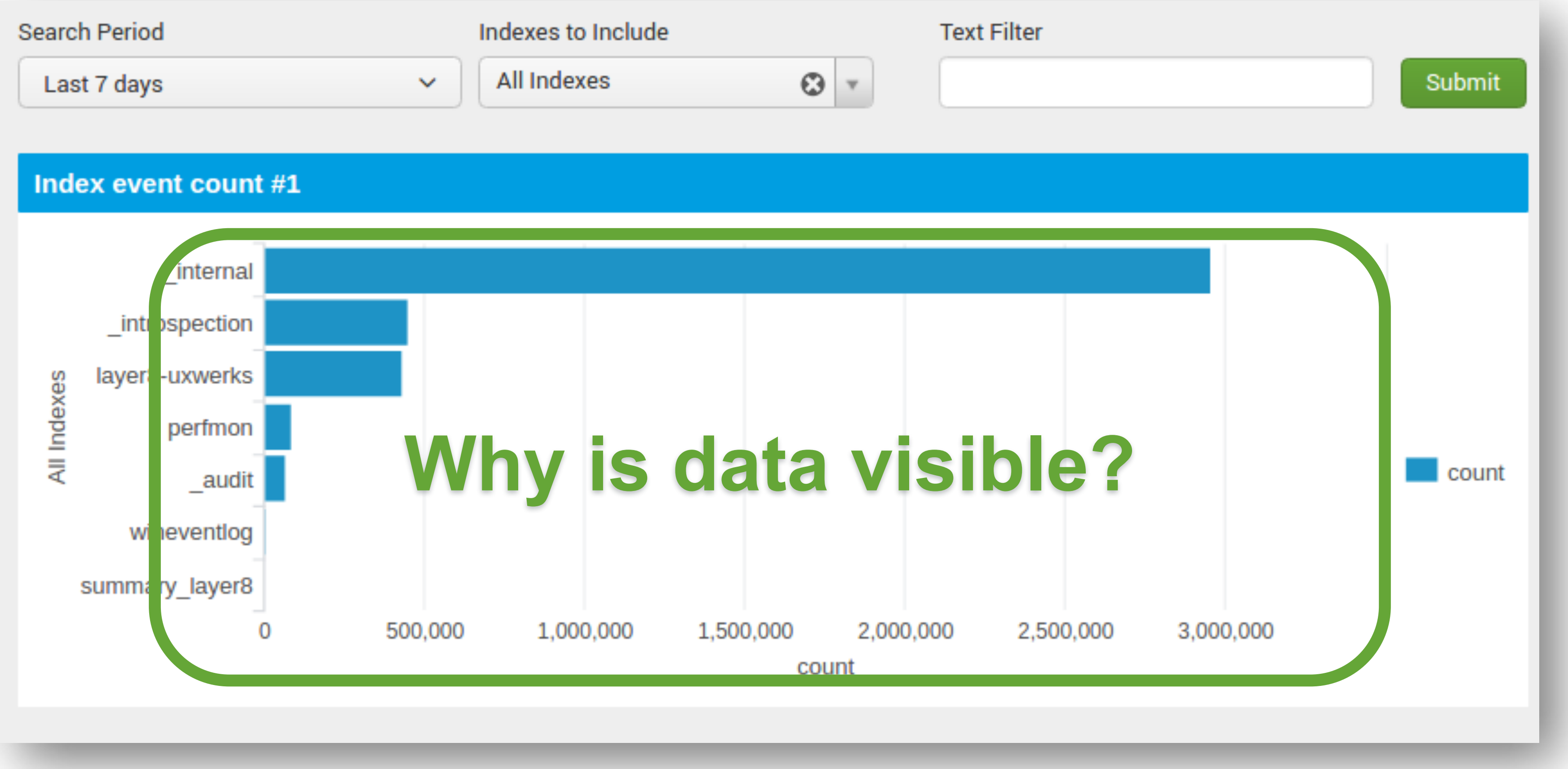
As of Splunk 6.6, empty text inputs do not default to undefined



Text Input Tokens

Empty values are not undefined

As of Splunk 6.6, empty text inputs do not default to undefined



Search Period: Last 7 days

Indexes to Include: All Indexes

Text Filter:

Submit

Index event count #1

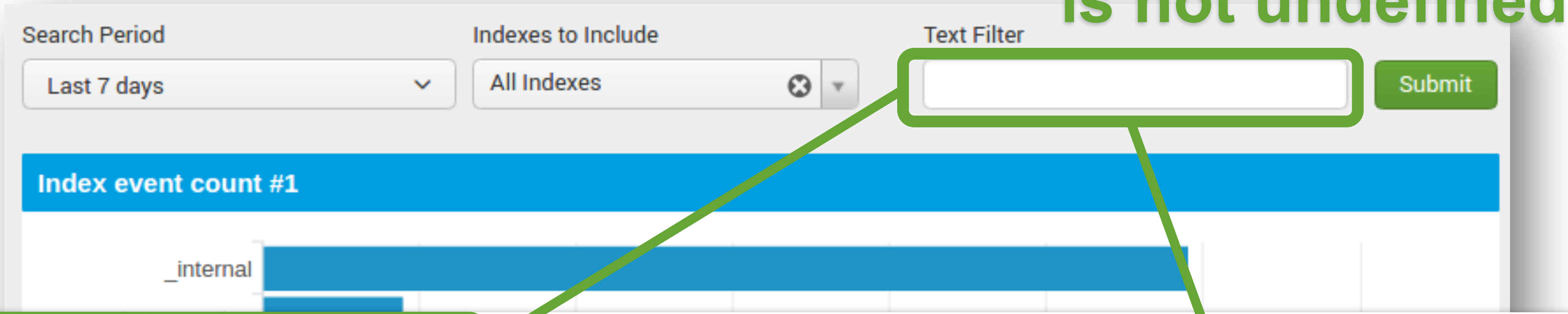
Why is data visible?

Text Input Tokens

Empty values are not undefined

As of Splunk 6.6, empty text inputs do not default to undefined

“” is not undefined

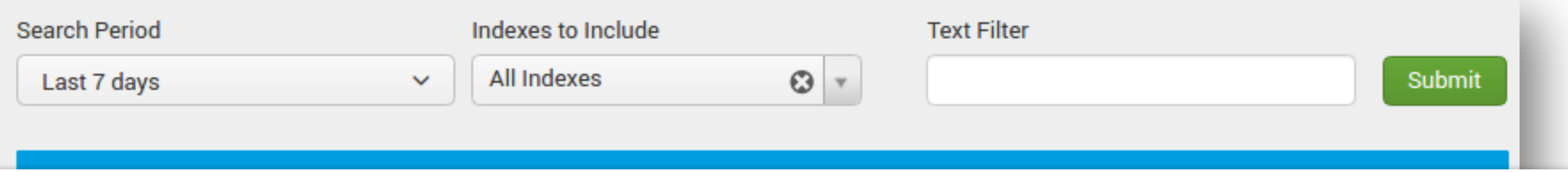


```
<panel depends="$text_filter$">
  <chart>
      <title>Index event count #1</title>
      <search>
        <query>
          | tstats count where index=$index_filters$ TERM($text_filter$) by index
          | sort 10 -count
        </query>
      </search>
```

Text Input Tokens

Empty values are not undefined

As of Splunk 6.6, empty text inputs do not default to undefined



Search Period: Last 7 days

Indexes to Include: All Indexes

Text Filter:

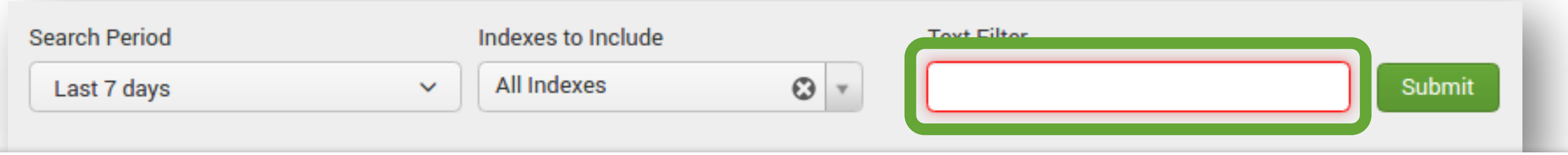
Use SimpleXML to cleanup an empty value

```
<input type="text" token=“text_filter" searchWhenChanged="false">
  <label>Text Filter</label>
  <change>
    <condition match="isnotnull('value') AND
          (len('value') == 0 OR match('value', &quot;^\\s+$&quot;))">
      <unset token="form.text_filter"/>
    </condition>
  </change>
</input>
```

Text Input Tokens

Empty values are not undefined

As of Splunk 6.6, empty text inputs do not default to undefined



Search Period: Last 7 days

Indexes to Include: All Indexes

Text Filter:

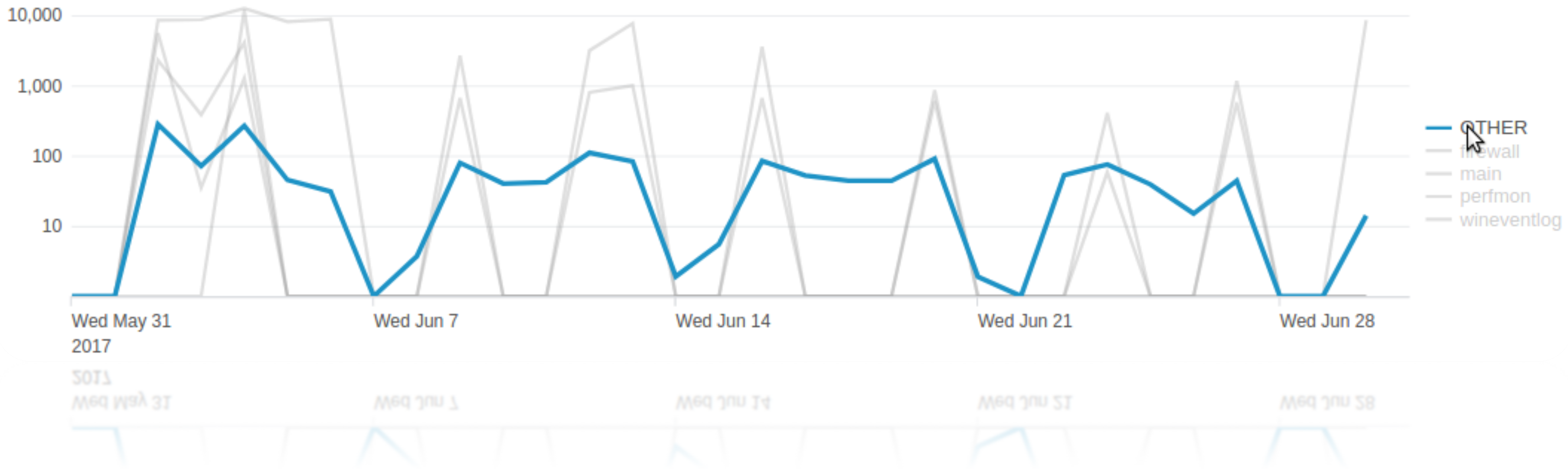
Use JS to clean and highlight inputs

```
defaultTokens.on("change:text_filter", function(model, value, options) {
  if (typeof value !== 'undefined' && value.replace(/\s/g,"") === "") {
    setToken("form.text_filter", undefined);
  } else if (typeof value !== 'undefined') {
    setToken("form.text_filter", value.trim());
  }
  checkEmptyTokenFocusForDashboard(["text_filter"]);
});
```

Smarter Chart Drilldowns

Filtering out unwanted drilldown methods

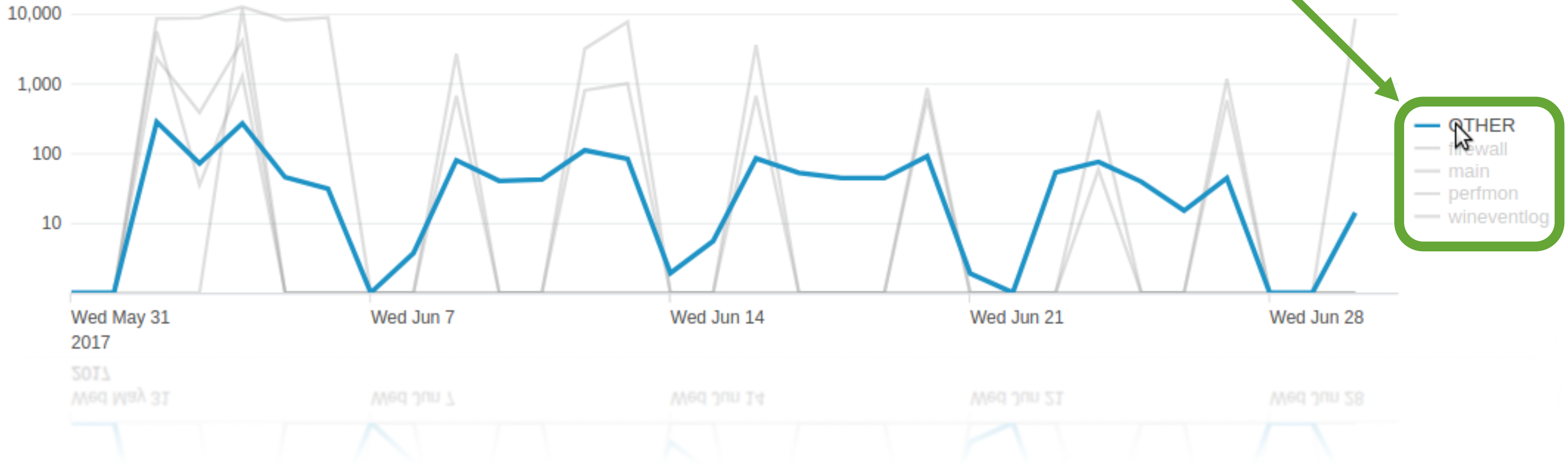
As of Splunk 6.3, you can prevent drilldowns from the legend in SimpleXML



Smarter Chart Drilldowns

Filtering out unwanted drilldown methods

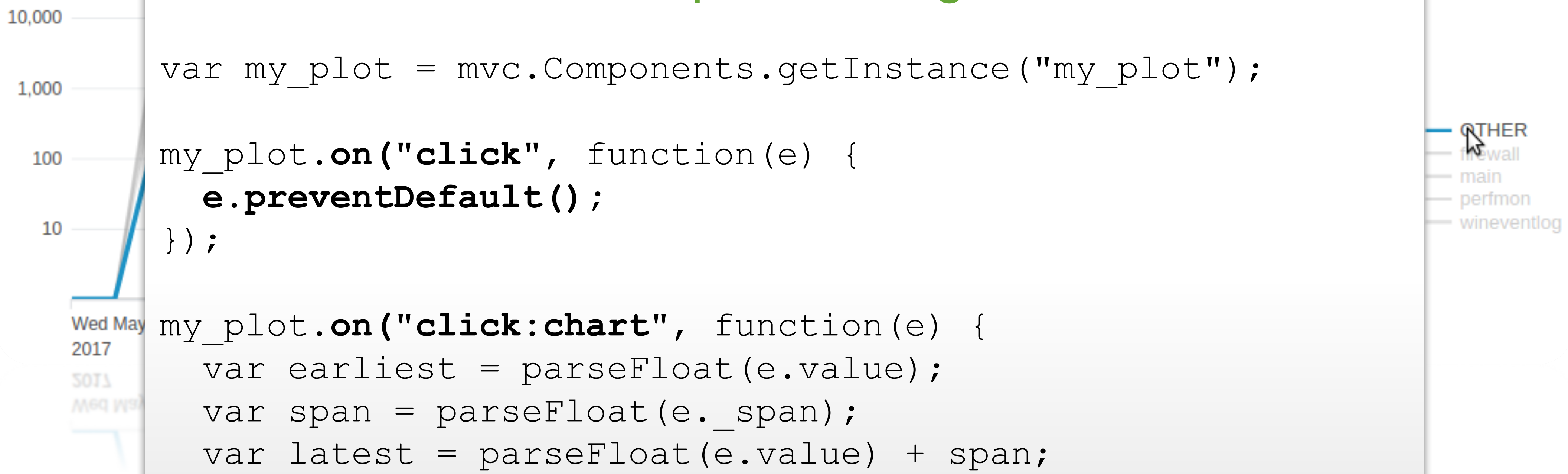
As of Splunk 6.3, you can prevent drilldowns from the legend in SimpleXML



Smarter Chart Drilldowns

Filtering out unwanted drilldown methods

As of Splunk 6.3, you can prevent drilldowns from the legend in SimpleXML



Old JS method to prevent legend drilldowns

```
var my_plot = mvc.Components.getInstance("my_plot");

my_plot.on("click", function(e) {
  e.preventDefault();
});

my_plot.on("click:chart", function(e) {
  var earliest = parseFloat(e.value);
  var span = parseFloat(e._span);
  var latest = parseFloat(e.value) + span;
  var drilldown_val = e.name2;
  …
});
```

Smarter Chart Drilldowns

Filtering out unwanted drilldown methods

As of Splunk 6.3, you can prevent drilldowns from the legend in SimpleXML

SimpleXML to prevent legend drilldowns for timecharts

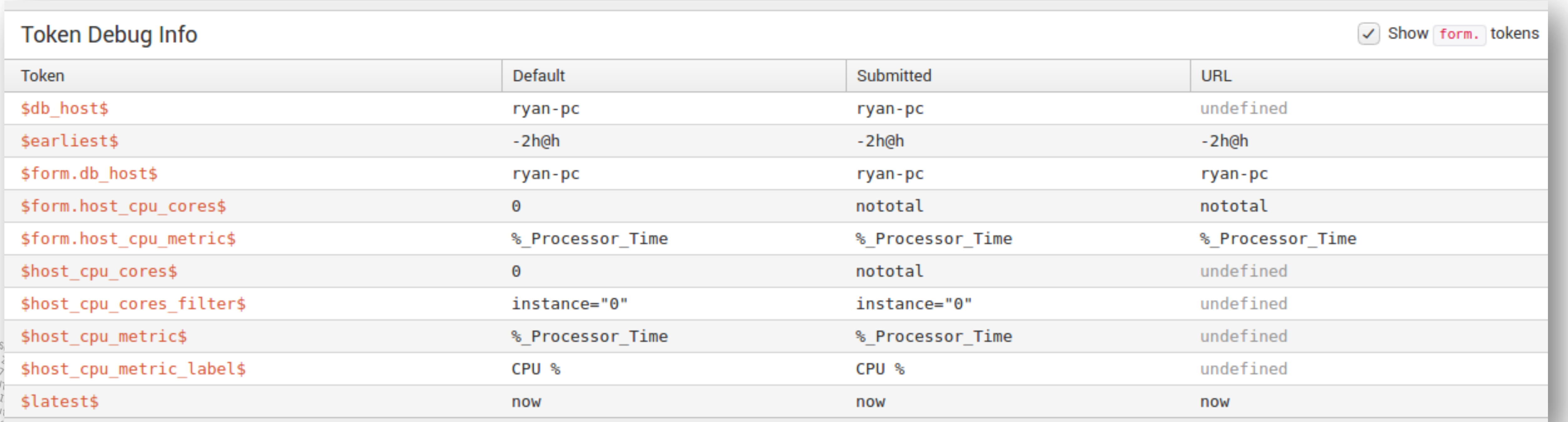
```
<drilldown target="_blank">
  <condition match="isnotnull('row._span')">
    <eval token="earliest_dd">$earliest$ - $row._span$</eval>
    <eval token="latest_dd">$latest$ + $row._span$</eval>
    <link><![CDATA[ … ]]></link>
  </condition>
  <condition></condition>
</drilldown>
```

Passing Tokens In URL

Creating static, one-time use tokens

Another token model, the URL token model, reflects what you see in the address bar of the dashboard

```
…?earliest=-2h%40h&latest=now&form.host_cpu_metric=%25_Processor_Time
&form.host_cpu_cores=nototal&form.db_host=ryan-pc
```



Token Debug Info

☑ Show form. tokens

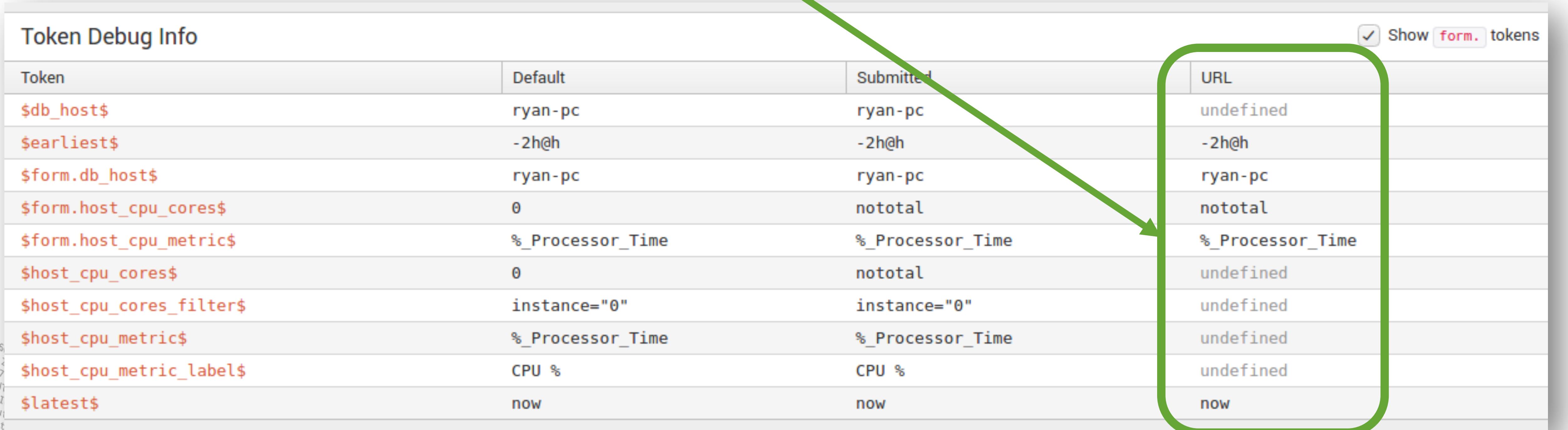
Token	Default	Submitted	URL
db_host	ryan-pc	ryan-pc	undefined
$earliest$	-2h@h	-2h@h	-2h@h
$form.db_host$	ryan-pc	ryan-pc	ryan-pc
$form.host_cpu_cores$	0	nototal	nototal
$form.host_cpu_metric$	%_Processor_Time	%_Processor_Time	%_Processor_Time
$host_cpu_cores$	0	nototal	undefined
$host_cpu_cores_filter$	instance="0"	instance="0"	undefined
$host_cpu_metric$	%_Processor_Time	%_Processor_Time	undefined
$host_cpu_metric_label$	CPU %	CPU %	undefined
$latest$	now	now	now

Passing Tokens In URL

Creating static, one-time use tokens

Another token model, the URL token model, reflects what you see in the address bar of the dashboard

```
…?earliest=-2h%40h&latest=now&form.host_cpu_metric=%25_Processor_Time
&form.host_cpu_cores=nototal&form.db_host=ryan-pc
```



Token Debug Info

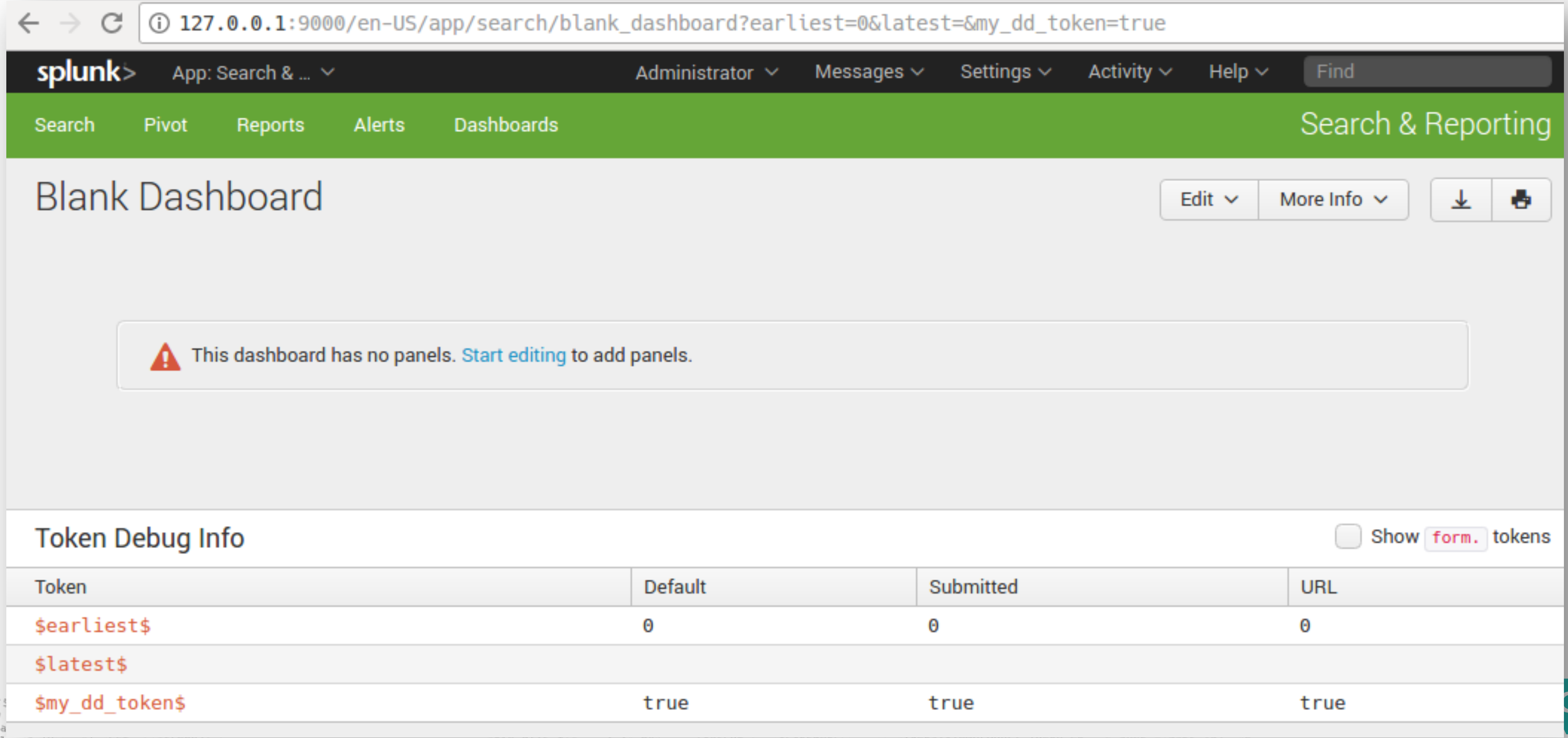
☑ Show form. tokens

Token	Default	Submitted	URL
db_host	ryan-pc	ryan-pc	undefined
$earliest$	-2h@h	-2h@h	-2h@h
$form.db_host$	ryan-pc	ryan-pc	ryan-pc
$form.host_cpu_cores$	0	nototal	nototal
$form.host_cpu_metric$	%_Processor_Time	%_Processor_Time	%_Processor_Time
$host_cpu_cores$	0	nototal	undefined
$host_cpu_cores_filter$	instance="0"	instance="0"	undefined
$host_cpu_metric$	%_Processor_Time	%_Processor_Time	undefined
$host_cpu_metric_label$	CPU %	CPU %	undefined
$latest$	now	now	now

Passing Tokens In URL

Creating static, one-time use tokens

Adding a token to the URL will make it appear in the dashboard



```
127.0.0.1:9000/en-US/app/search/blank_dashboard?earliest=0&latest=&my_dd_token=true
```

Blank Dashboard

This dashboard has no panels. Start editing to add panels.

Token Debug Info

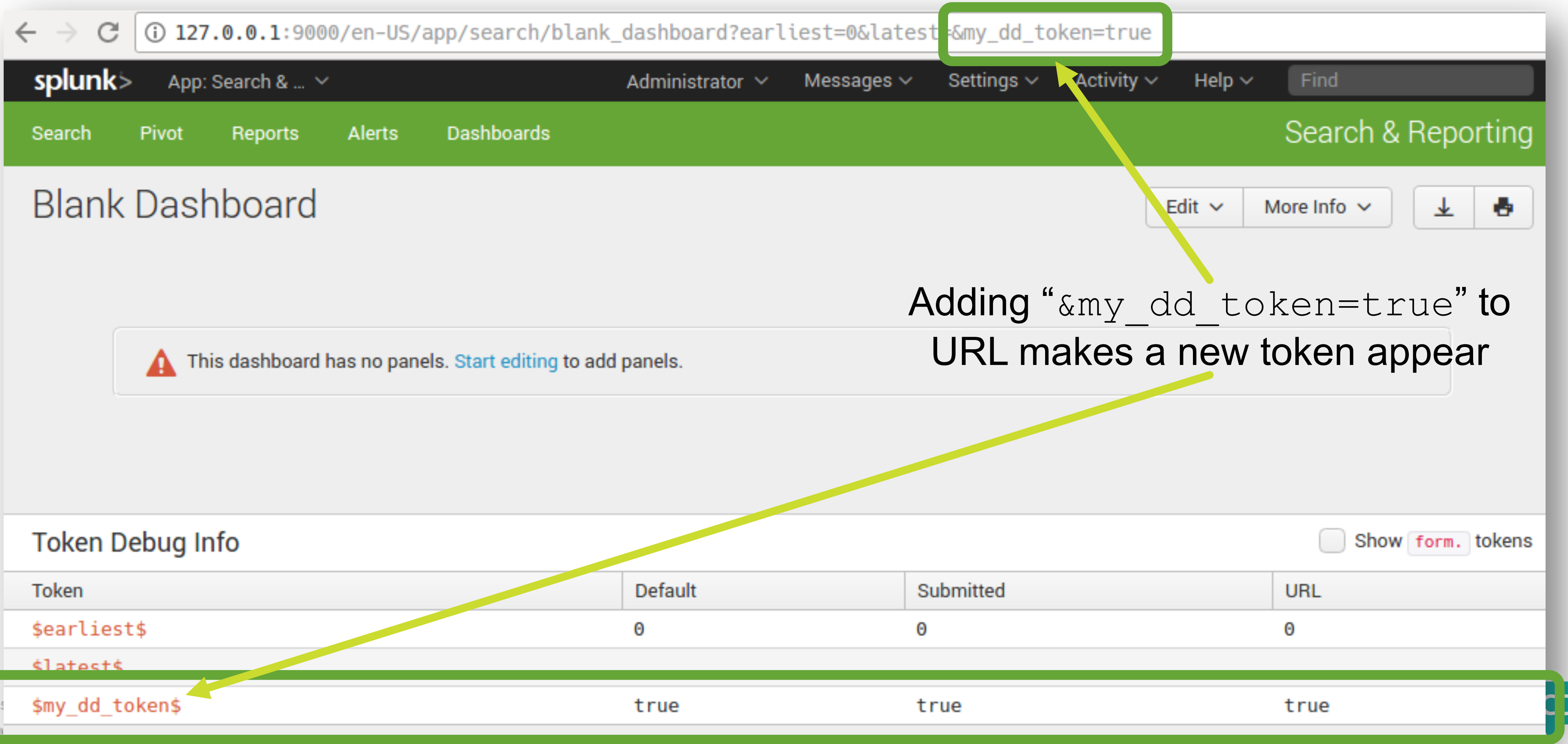
□ Show form. tokens

Token	Default	Submitted	URL
$earliest$	0	0	0
$latest$			
my_dd_token	true	true	true

Passing Tokens In URL

Creating static, one-time use tokens

Adding a token to the URL will make it appear in the dashboard



```
127.0.0.1:9000/en-US/app/search/blank_dashboard?earliest=0&latest&my_dd_token=true
```

Blank Dashboard

This dashboard has no panels. Start editing to add panels.

Token Debug Info

□ Show form. tokens

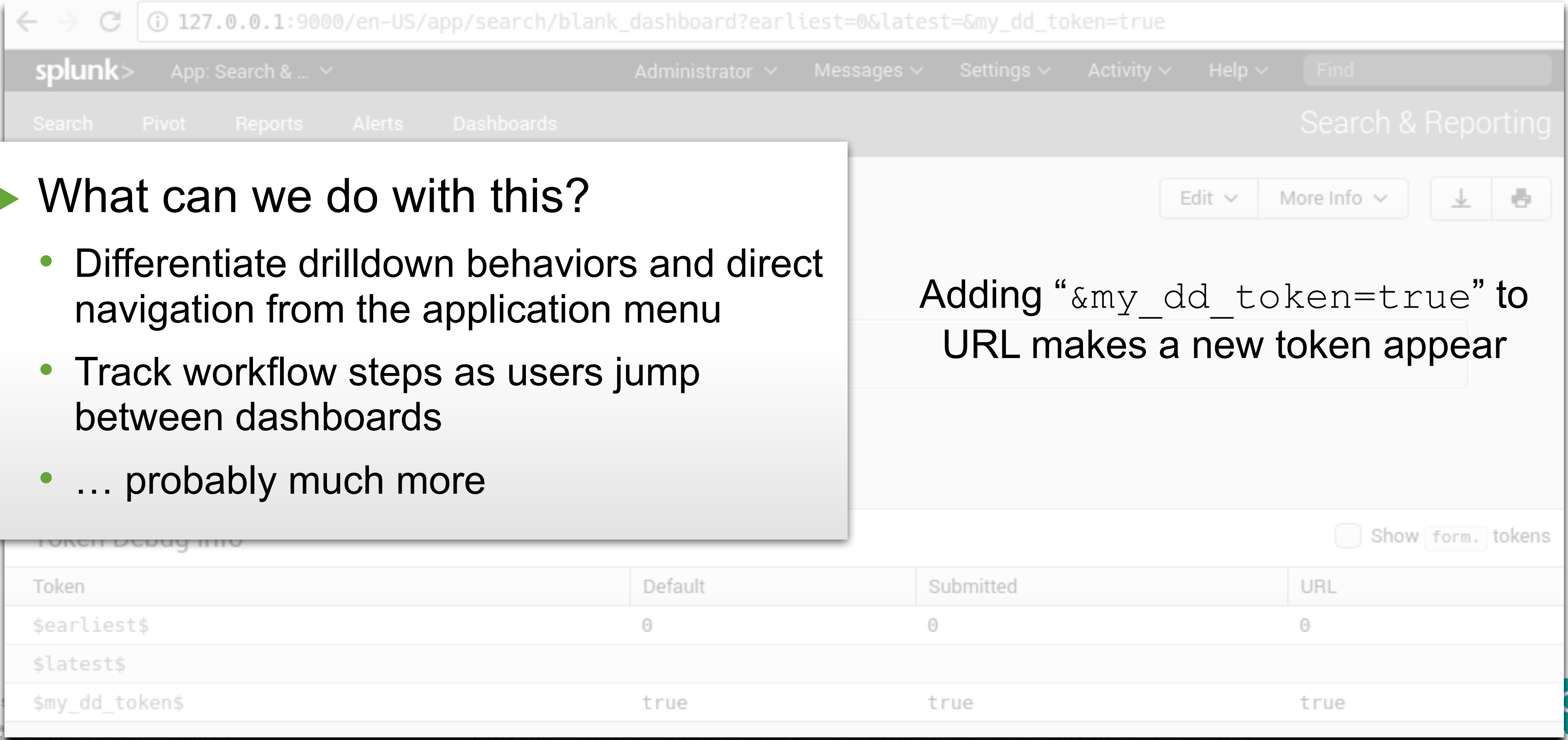
Token	Default	Submitted	URL
$earliest$	0	0	0
$latest$			
my_dd_token	true	true	true

Adding “&my_dd_token=true” to URL makes a new token appear

Passing Tokens In URL

Creating static, one-time use tokens

Adding a token to the URL will make it appear in the dashboard



```
127.0.0.1:9000/en-US/app/search/blank_dashboard?earliest=0&latest=&my_dd_token=true
```

- What can we do with this?
  - Differentiate drilldown behaviors and direct navigation from the application menu
  - Track workflow steps as users jump between dashboards
  - … probably much more

Adding “&my_dd_token=true” to URL makes a new token appear

Token Debug Info

Token	Default	Submitted	URL
$earliest$	0	0	0
$latest$			
my_dd_token	true	true	true

Safe, Inert Token Values

Using whitespace as the token value

Whitespace token values can help limit side-effects in searches, i.e., use of unnecessary pipeline steps or Boolean conditions

Ever try to do this: `<set token="my_token"> </set>`

… and encounter weird editing issues?

Use this instead: `<set token="my_token">&#32;</set>`

`&#32;` is the HTML entity for the space character (hitting spacebar) and generally safer / more resilient to editor side-effects

Safe, Inert Token Values …

Using a whitespace token in a SPL query

Whitespace token values can help limit side-effects in searches, like this example where we prioritize three searches in a dashboard

```
<search>
  <query>HIGH Priority Search #1 …</query>
  <progress>
    <unset token="seach_1_done"/>
  </progress>
  <done>
    <set token="seach_1_done">&#32;</set>
  </done>
</search>
```

See @woodcock answer at https://answers.splunk.com/answers/513660/how-to-set-loading-order-for-panels.html

Safe, Inert Token Values …

Using a whitespace token in a SPL query

Whitespace token values can help limit side-effects in searches, like this example where we prioritize three searches in a dashboard

```
<search>
  <query>HIG
  <progress>
    <unset t
  </progress
  <done>
    <set tok
  </done>
</search>
```

```
<search>
  <query>HIGH Priority Search #2 …</query>
  <progress>
    <unset token="seach_2_done"/>
  </progress>
  <done>
    <set token="seach_2_done">&#32;</set>
  </done>
</search>
```

See @woodcock answer at https://answers.splunk.com/answers/513660/how-to-set-loading-order-for-panels.html

Safe, Inert Token Values …

Using a whitespace token in a SPL query

Whitespace token values can help limit side-effects in searches, like this example where we prioritize three searches in a dashboard

```
<search>
  <query>HIG
  <progress>
    <unset t
  </progress
  <done>
    <set tok
  </done>
</search>
```

```
<search>
  <query>HIG
  <progress>
    <unset t
  </progress
  <done>
    <set tok
  </done>
</search>
```

```
<search>
  <query>HIGH Priority Search #3 …</query>
  <progress>
    <unset token="seach_3_done"/>
  </progress>
  <done>
    <set token="seach_3_done">&#32;</set>
  </done>
</search>
```

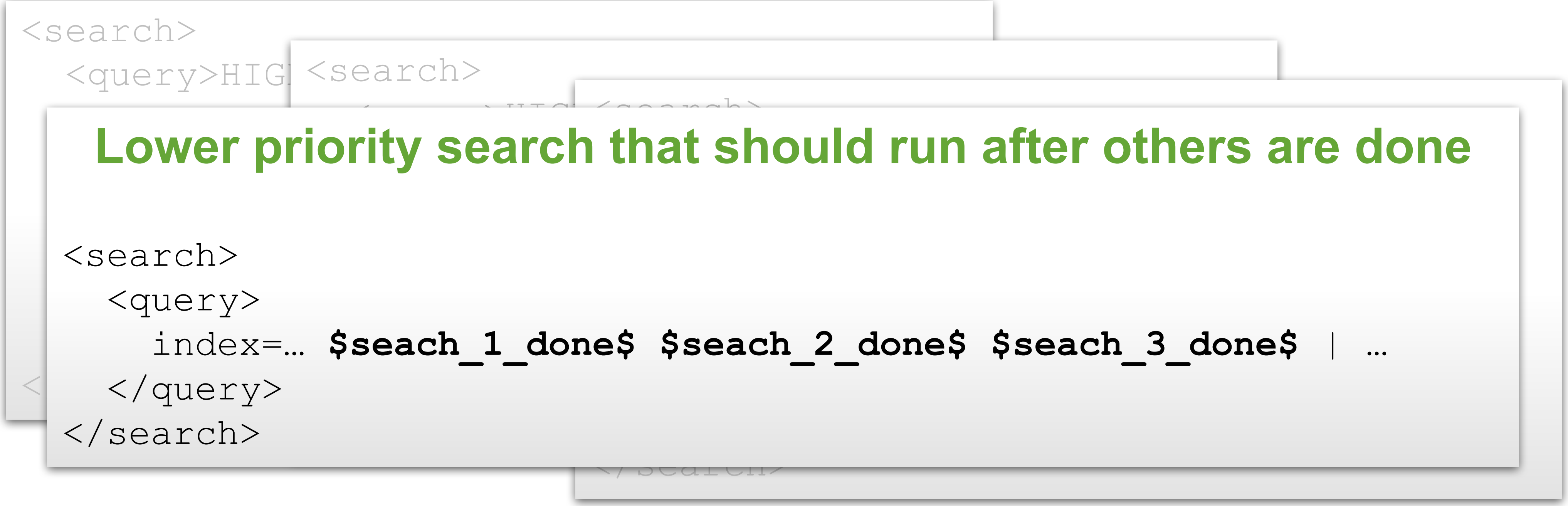
See @woodcock answer at https://answers.splunk.com/answers/513660/how-to-set-loading-order-for-panels.html

splunk> .conf2017

Safe, Inert Token Values …

Using a whitespace token in a SPL query

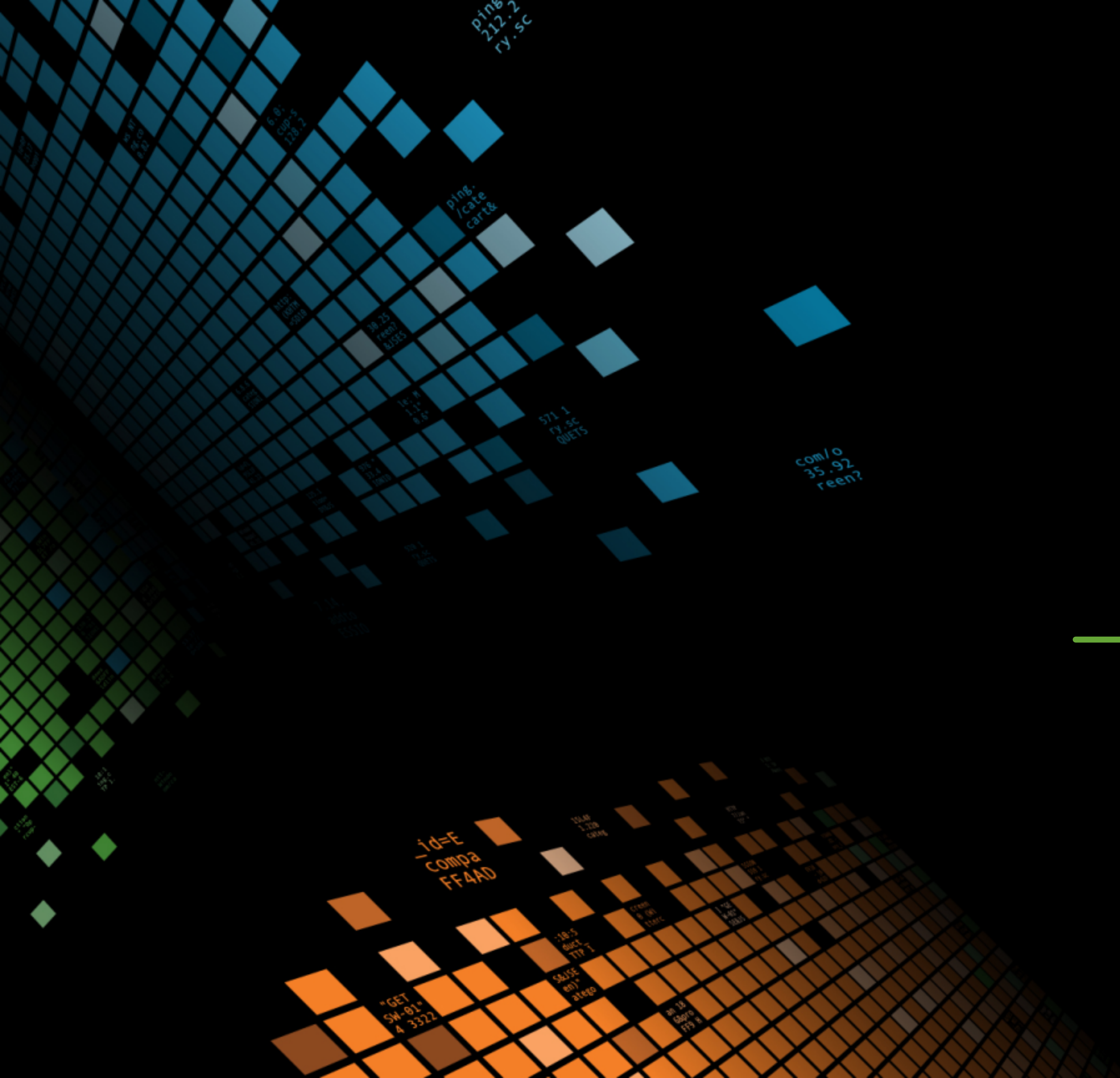
Whitespace token values can help limit side-effects in searches, like this example where we prioritize three searches in a dashboard



Lower priority search that should run after others are done

```
<search>
  <query>
    index=… $seach_1_done$ $seach_2_done$ $seach_3_done$ | …
  </query>
</search>
```

See @woodcock answer at https://answers.splunk.com/answers/513660/how-to-set-loading-order-for-panels.html



Wrapping Up

Token Models

How tokens are managed

Data structures that **record** the **token names** and **values**, driving dashboard behaviors as values change

- **Default** token model
  - Current value of any input
  - Populating searches for inputs are triggered by changes in this model
  - Can manipulate values of non-input tokens only in JS, i.e., SimpleXML changes affect both Default and Submitted token models
  - Not related to `<init>` element, which is used to set initial values of tokens

- **Submitted** token model
  - Values when “Submit” event occurs
  - Ad-hoc / base / panel searches are triggered by changes in this model
  - Panel visibility (`depends="$…$"` and `rejects="$…$"`) is based on this model
  - Can manipulate values of non-input tokens directly in SimpleXML

Last Token Tidbits

- SimpleXML token-related behaviors can be overwritten by JS
  - Custom token change handlers
  - Search update / refresh behaviors

- Never use a token in the definition of an input property or another token value … will not update values like you want
  - `<valuePrefix>$my_field$=</valuePrefix>`
  - `<set token="my_query">index=foo host=$bar$</set>`

- The `depends="…"` and `rejects="…"` visualization controls do not affect populating searches, i.e., a panel’s search updates regardless of the panel’s visibility

- Use unique search terms to find documentation, e.g., “unset”, “search event handlers”, “token models”, etc.

Wrapping Up

- Tokens are like variables for dashboards
- Understanding how to use tokens effectively can drastically improve dashboard efficiency and UX
- Use the token debugger to expedite development and troubleshooting
- App developers need to be aware of when token-related features evolve in SimpleXML

Thank You

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

splunk> .conf2017

Sign-Off

- Track me down in person or in the digital Splunk community if you want to learn more and discuss things
  - Blog: https://blog.octoinsight.com/tag/splunk
  - Splunk Answers: @rjthibod
  - Splunk Slack: @artie73
- The **Layer8Insight App for Splunk** is my app that uses many of the techniques presented in this session. Feel free to use as a reference

Other .conf Sessions

- The Art of Detection Using Splunk Enterprise Security, Douglass Brown, Wednesday 4:35pm
- Beyond REGULAR Regular Expressions v2.0, Cary Peterrborg, Wednesday 4:35pm.
- Splunking Splunkbase for App Development Recommendations, Thursday 10:30am
- Splunk Reactions Tumblr, Dave Shipritz, Wednesday 12:15pm
- Literal Data Fabrics: The Splunk Gallery, Charlie Huggard, Wednesday 2:45pm

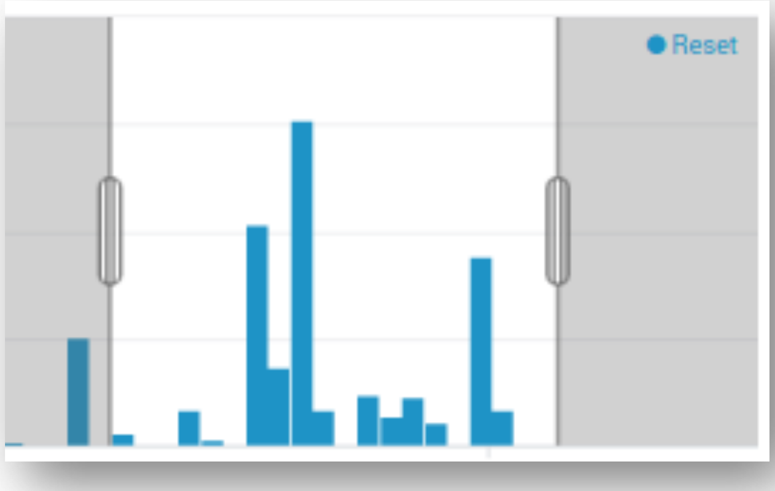
Appendix

- There are more examples / slides for your learning pleasure

Pan & Zoom Time-Selection

Default is set to parent search time

As of Splunk 6.6, pan & zoom time selection is always set to parent search time



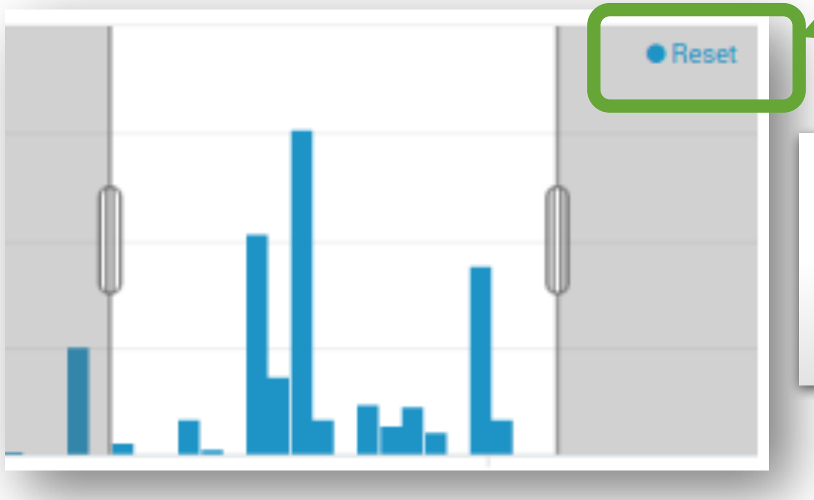
```
<selection>
  <set token="time_dd_select.earliest">$start$</set>
  <set token="time_dd_select.latest">$end$</set>
</selection>
```

The values for $start$ and $end$ are still set when pan & zoom is not in use, i.e., your drilldown will search will still run

Pan & Zoom Time-Selection

Default is set to parent search time

As of Splunk 6.6, pan & zoom time selection is always set to parent search time



Spy on this to detect pan & zoom

```
<selection>
  <set token="time_dd_select.earliest">$start$</set>
  <set token="time_dd_select.latest">$end$</set>
</selection>
```

The values for $start$ and $end$ are still set when pan & zoom is not in use, i.e., your drilldown will search will still run

Pan & Zoom Time-Selection

Spying on the Reset button

Detect changes to selection tokens and set timer to evaluate state

```
defaultTokenModel.on("change:time_dd_select.earliest", …) {
  setPanZoomTimer();
});
defaultTokenModel.on("change:time_dd_select.latest", …) {
  setPanZoomTimer();
});
```

Set the drilldown time tokens only if the Reset button is present

```
// callback for setPanZoomTimer timer expiration
function checkPanZoomBoundaries() {
  var ts_earliest = getToken("time_dd_select.earliest");
  var ts_latest   = getToken("time_dd_select.latest");

  if ($(“#chart_id_plot”).find('[class*="btn-reset"]').length {
    setToken("form.dd_time.earliest", ts_earliest);
    setToken("form.dd_time.latest", ts_latest);
    submitTokens();
  }
}
```

Predictable Checkbox Tokens

Forcing checkbox token value ordering

Checkbox tokens are ordered based on user selection

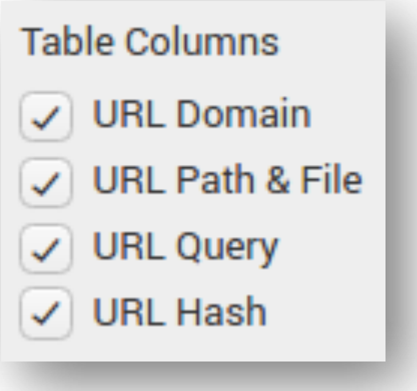


Table Columns

☑ URL Domain

☑ URL Path & File

☑ URL Query

☑ URL Hash

```
["url_domain","url_path_file","url_query","url_hash"]
```

Predictable Checkbox Tokens

Forcing checkbox token value ordering

Checkbox tokens are ordered based on user selection

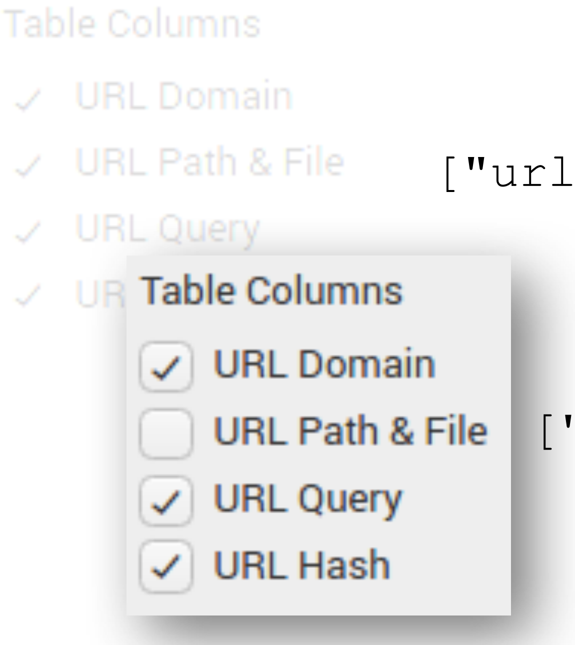


Table Columns

✓ URL Domain

✓ URL Path & File

✓ URL Query

✓ UR

```
["url_domain","url_path_file","url_query","url_hash"]
```

Table Columns

☑ URL Domain

□ URL Path & File

☑ URL Query

☑ URL Hash

```
["url_domain","url_query","url_hash"]
```

Predictable Checkbox Tokens

Forcing checkbox token value ordering

Checkbox tokens are ordered based on user selection

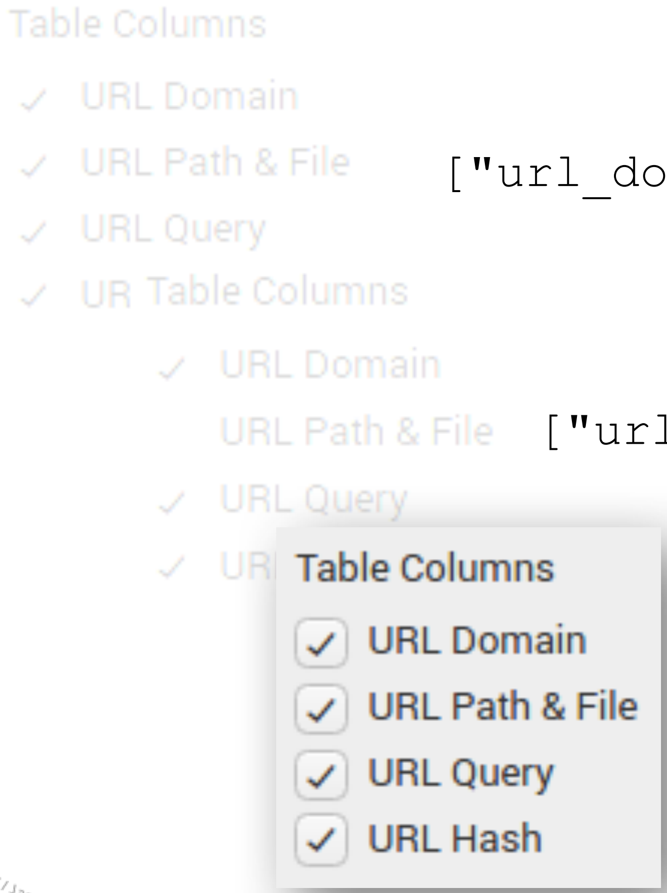


Table Columns

- ✓ URL Domain
- ✓ URL Path & File
- ✓ URL Query
- ✓ UR

```
["url_domain","url_path_file","url_query","url_hash"]
```

Table Columns

- ✓ URL Domain
- URL Path & File
- ✓ URL Query
- ✓ UR

```
["url_domain","url_query","url_hash"]
```

Table Columns

- ☑ URL Domain
- ☑ URL Path & File
- ☑ URL Query
- ☑ URL Hash

```
["url_domain","url_query","url_hash","url_path_file"]
```

Predictable Checkbox Tokens

Forcing checkbox token value ordering

Checkbox tokens are ordered based on user selection

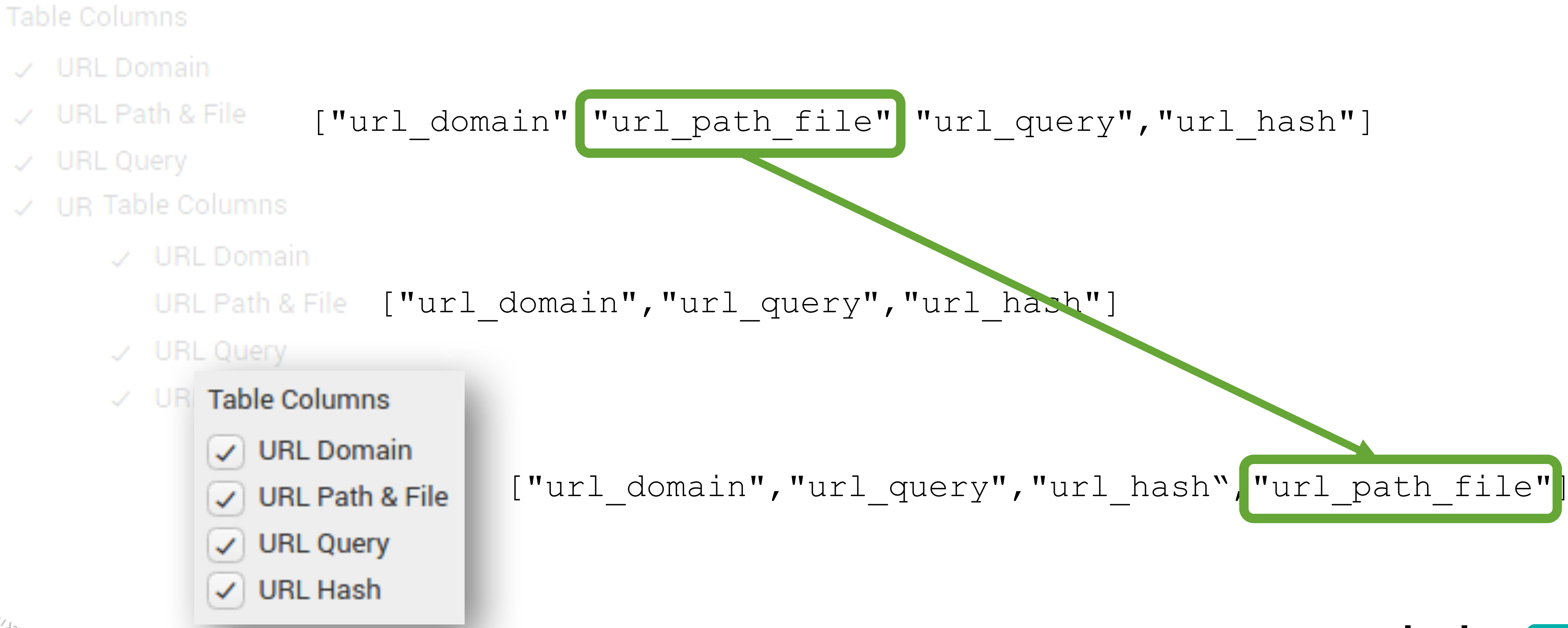


Table Columns

✓ URL Domain

✓ URL Path & File

✓ URL Query

✓ UR

```
["url_domain" "url_path_file" "url_query","url_hash"]
```

Table Columns

✓ URL Domain

URL Path & File

✓ URL Query

✓ UR

```
["url_domain","url_query","url_hash"]
```

Table Columns

☑ URL Domain

☑ URL Path & File

☑ URL Query

☑ URL Hash

```
["url_domain","url_query","url_hash“,"url_path_file"]
```

Predictable Checkbox Tokens

Forcing checkbox token value ordering

Checkbox tokens are ordered based on user selection

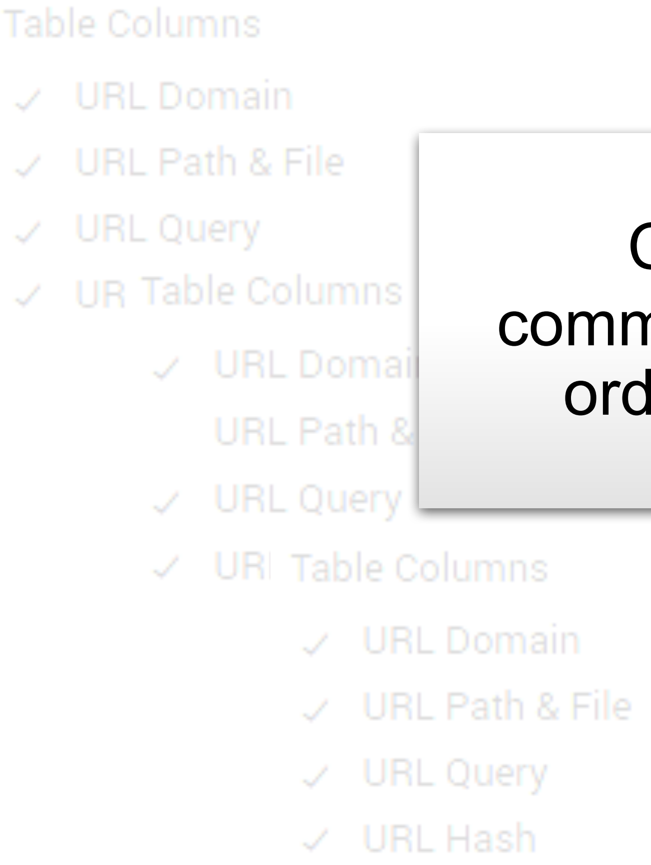


Table Columns

- ✓ URL Domain
- ✓ URL Path & File
- ✓ URL Query
- ✓ UR

Table Columns

- ✓ URL Domai
- URL Path &
- ✓ URL Query
- ✓ URL

Table Columns

- ✓ URL Domain
- ✓ URL Path & File
- ✓ URL Query
- ✓ URL Hash

h"]

Cannot naively use `fields` or `table` commands to produce result columns in a strict order, e.g., `| table $url_dim_token$`

```
["url_domain","url_query","url_hash“,"url_path_file"]
```

Predictable Checkbox Tokens

Forcing checkbox token value ordering

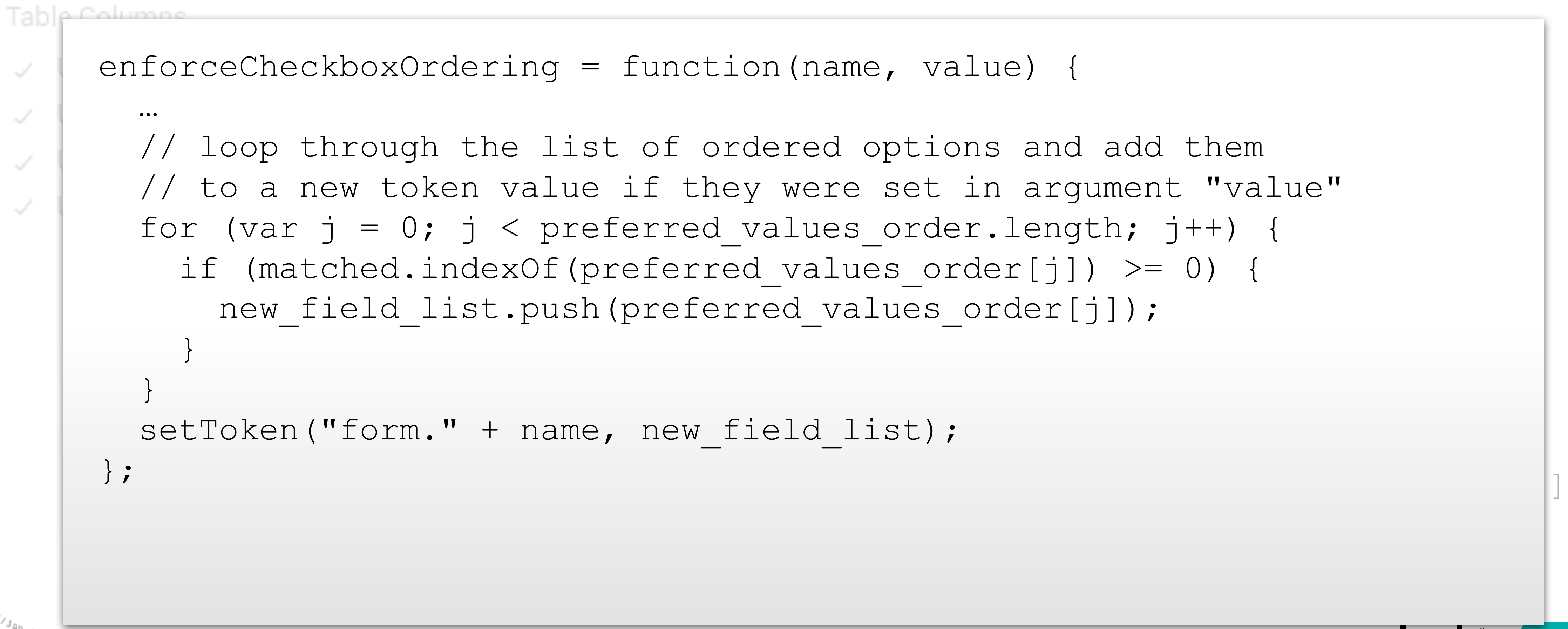
JS extension can enforce checkbox token order

```
enforceCheckboxOrdering = function(name, value) {
  var preferred_values_order = [], new_field_list = [], matched = [];
  var cb = mvc.Components.getInstance(name);
  var choices = cb.options.choices;

  // get list of checkbox values from the defined XML entity
  for (var i = 0; i < choices.length; i++) {
    preferred_values_order.push(choices[i]['value']);
  }

  // filter out passed token values that aren’t valid
  matched = value.filter(function(x) {
     return preferred_values_order.indexOf(x) >= 0 });
  …
```

Predictable Checkbox Tokens

Forcing checkbox token value ordering

JS extension can enforce checkbox token order



```
enforceCheckboxOrdering = function(name, value) {
  …
  // loop through the list of ordered options and add them
  // to a new token value if they were set in argument "value"
  for (var j = 0; j < preferred_values_order.length; j++) {
    if (matched.indexOf(preferred_values_order[j]) >= 0) {
      new_field_list.push(preferred_values_order[j]);
    }
  }
  setToken("form." + name, new_field_list);
};
```