



splunk>

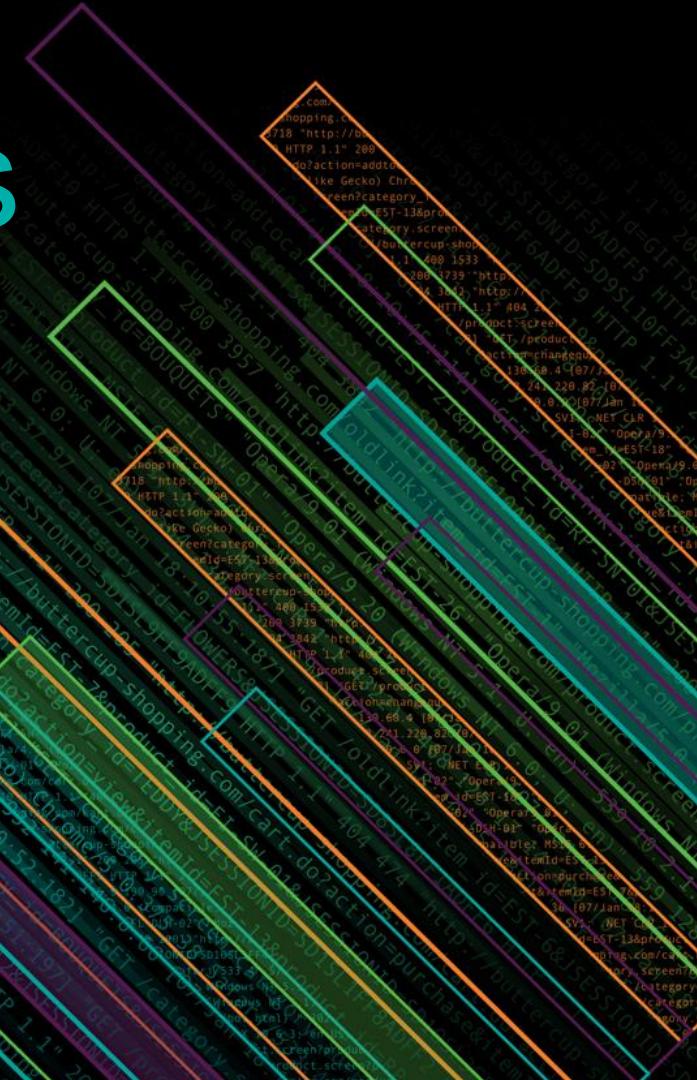
How We Track All Changes to Our Splunk Deployment

And what we learned along the way

Gabriel Vasseur - Thales UK - Senior cyber security analyst

Olivier Lauret - Octamis - Co-founder / Splunk Consultant

October 2018 | Version 12391784.3



Forward-Looking Statements

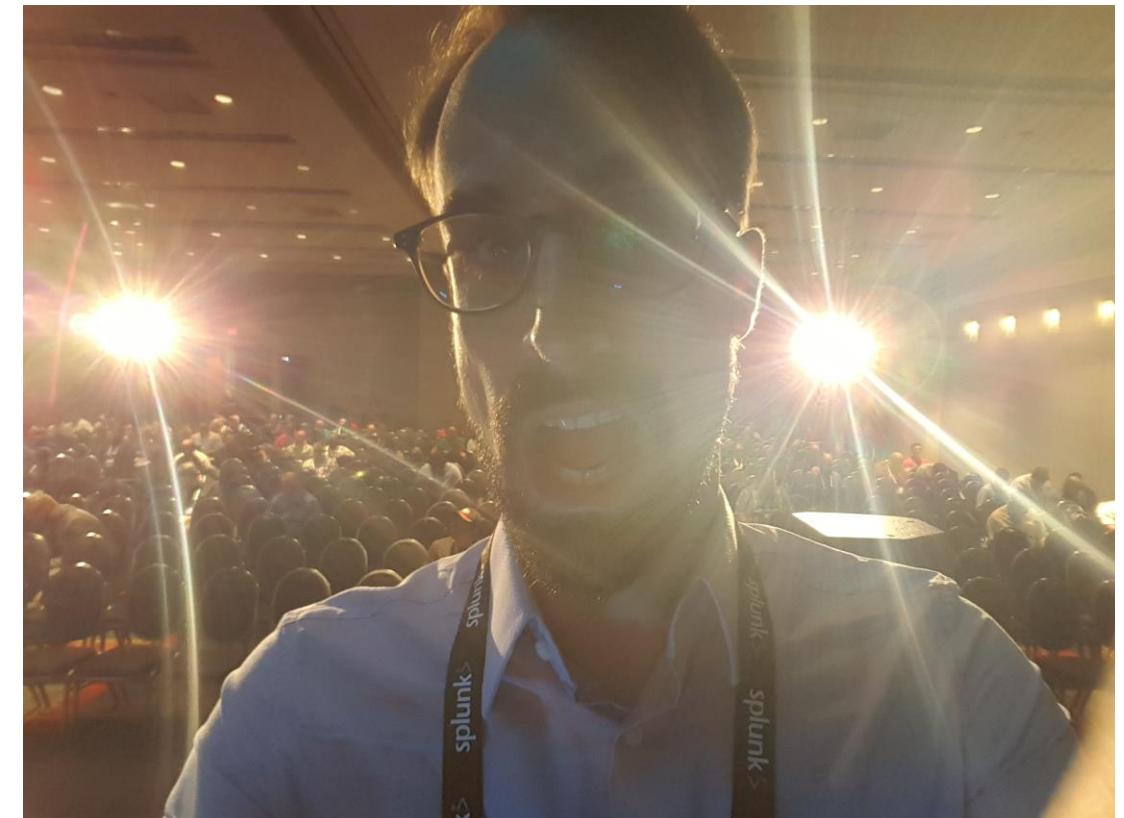
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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. © 2018 Splunk Inc. All rights reserved.

Who is Gabriel?

- ▶ French
- ▶ Lives in England
- ▶ PhD in theoretical physics
- ▶ Works for **THALES** UK
- ▶ 11 years in the IT security industry
- ▶ Currently
 - on paper: Senior Cyber Security Analyst
 - in reality: resident Data Scientist / Splunk Guru
- ▶ Likes to talk splunk
 - conf2016 [Become a Regular Expressions Ninja and Unlock Your Splunk Potential](#)
 - conf2017 [Running Enterprise Security at Capacity: Tuning ES With Data Model Acceleration](#)



→ one of the best-rated sessions!

Who is Olivier?

- ▶ French (guess where exactly from?) and British (100 years of fighting with myself)
- ▶ Based in Frankfurt, Germany

- ▶ Co-founder of **OCTAMIS** (UK, Germany)

Best company in the world (no doubt!)

- NMON/Metricator app

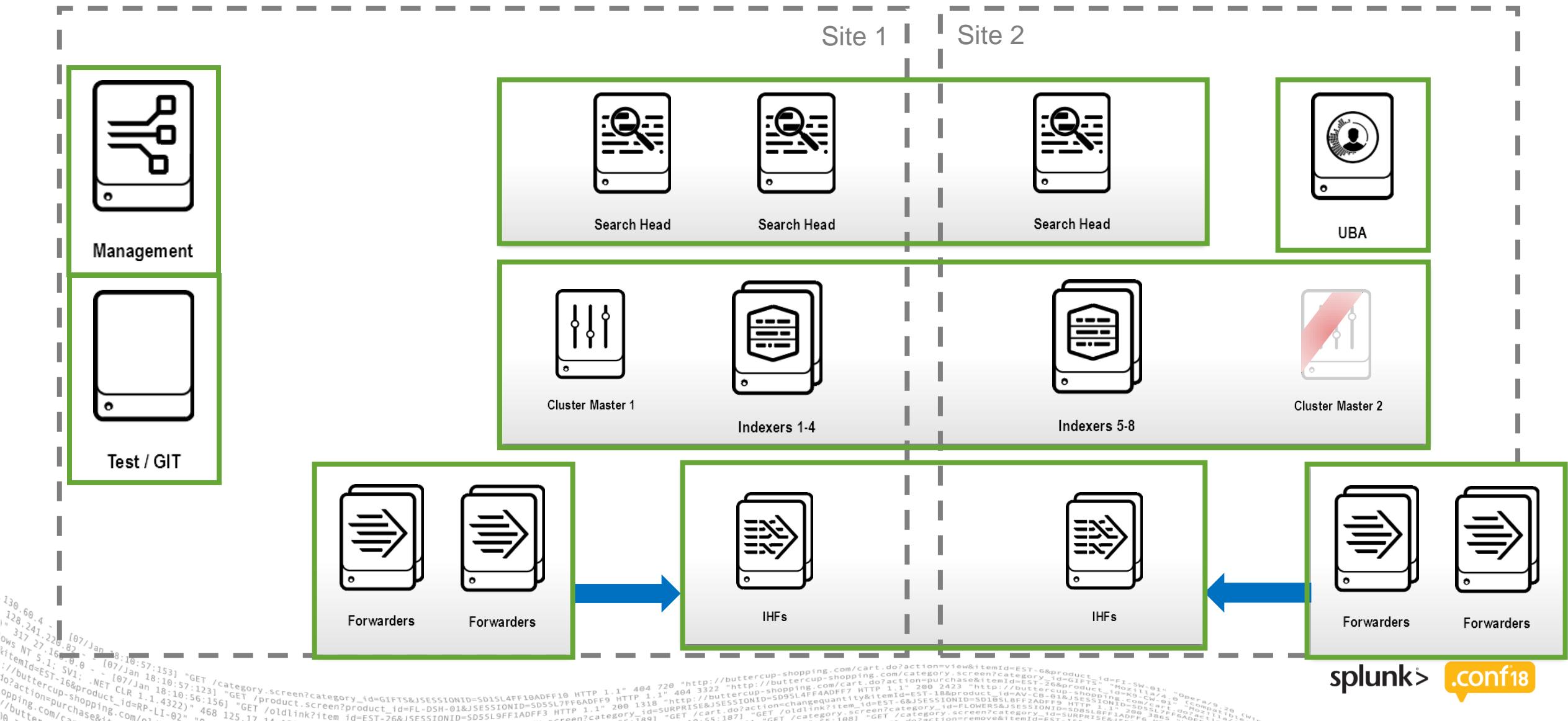


— Best App in the world (still not biased)

- ▶ Working as a Splunk consultant (looking for the next project!)
- ▶ 7+ years of passion with Splunk (many others with HP software, but let's not talk about the mistakes we did in our youth!)
- ▶ Some of you might recognise my voice from a Splunk Education class



Splunk at Thales UK





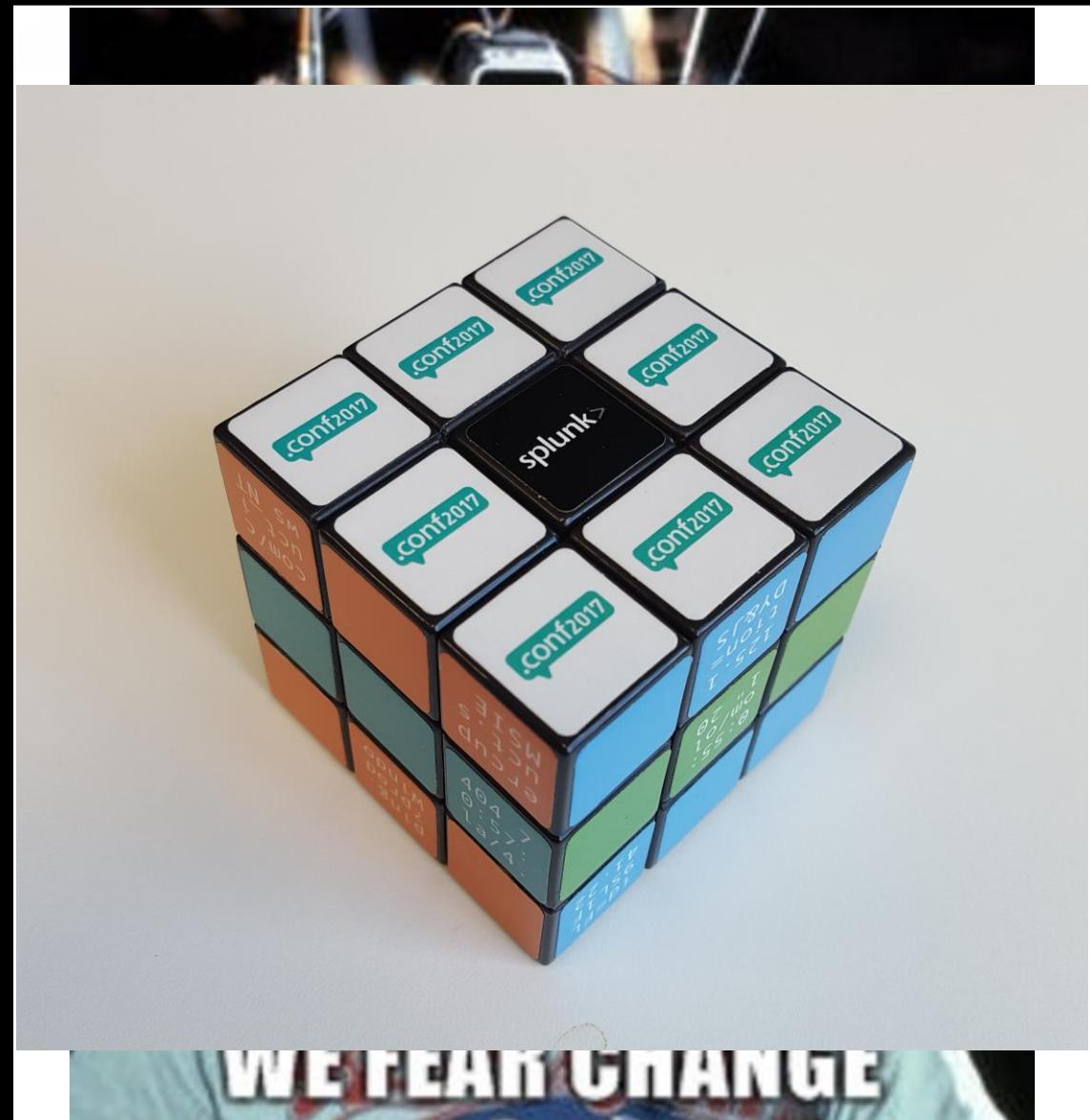
The one slide to photograph



- ▶ There will be subliminal information flashing on the screen, so watch the recording! <http://conf.splunk.com/sessions/2018-sessions.html>
- ▶ Your hosts:
 - Gabriel Vasseur gabriel.vasseur@uk.thalesgroup.com
<https://www.linkedin.com/in/gabrielvasseur/>
 - Olivier Lauret olivier@octamis.com
<https://www.linkedin.com/in/olivierlauret/>
- ▶ ! There are bonus slides :-)
- ▶ Slides and (a bit) more available now at <https://bit.ly/TrackSplunk>

The journey ahead

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ Tracking problem 1: precedence
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ Track all changes (inc. glass tables)
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades
- ▶ Conclusion



The journey ahead

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ Tracking problem 1: precedence
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ Track all changes (inc. glass tables)
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades

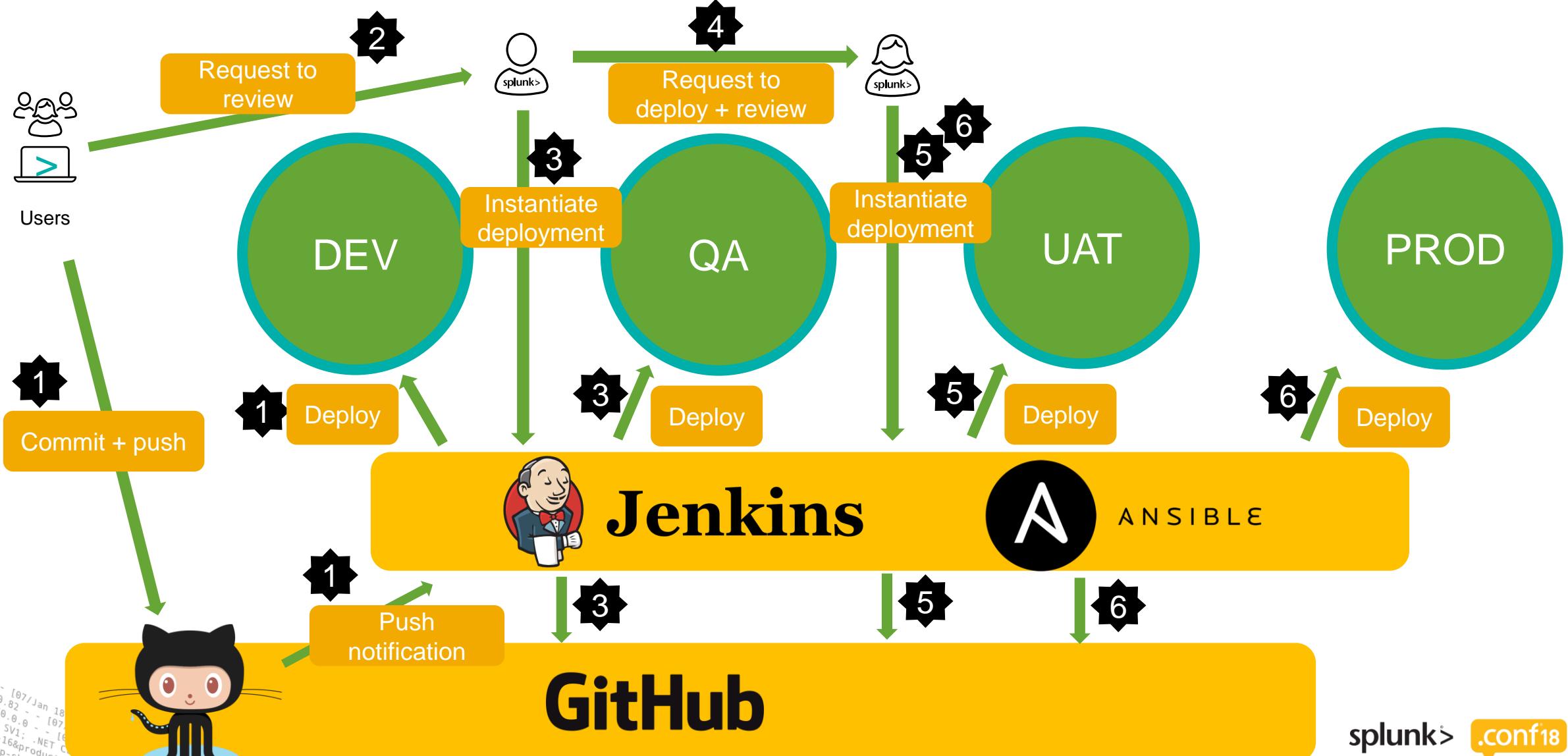


Proper Change Control is heavy



The heavy solution

Complete control on changes (NOT at Thales)



The heavy solution (Cont'd)

Complete control on changes

Advantages

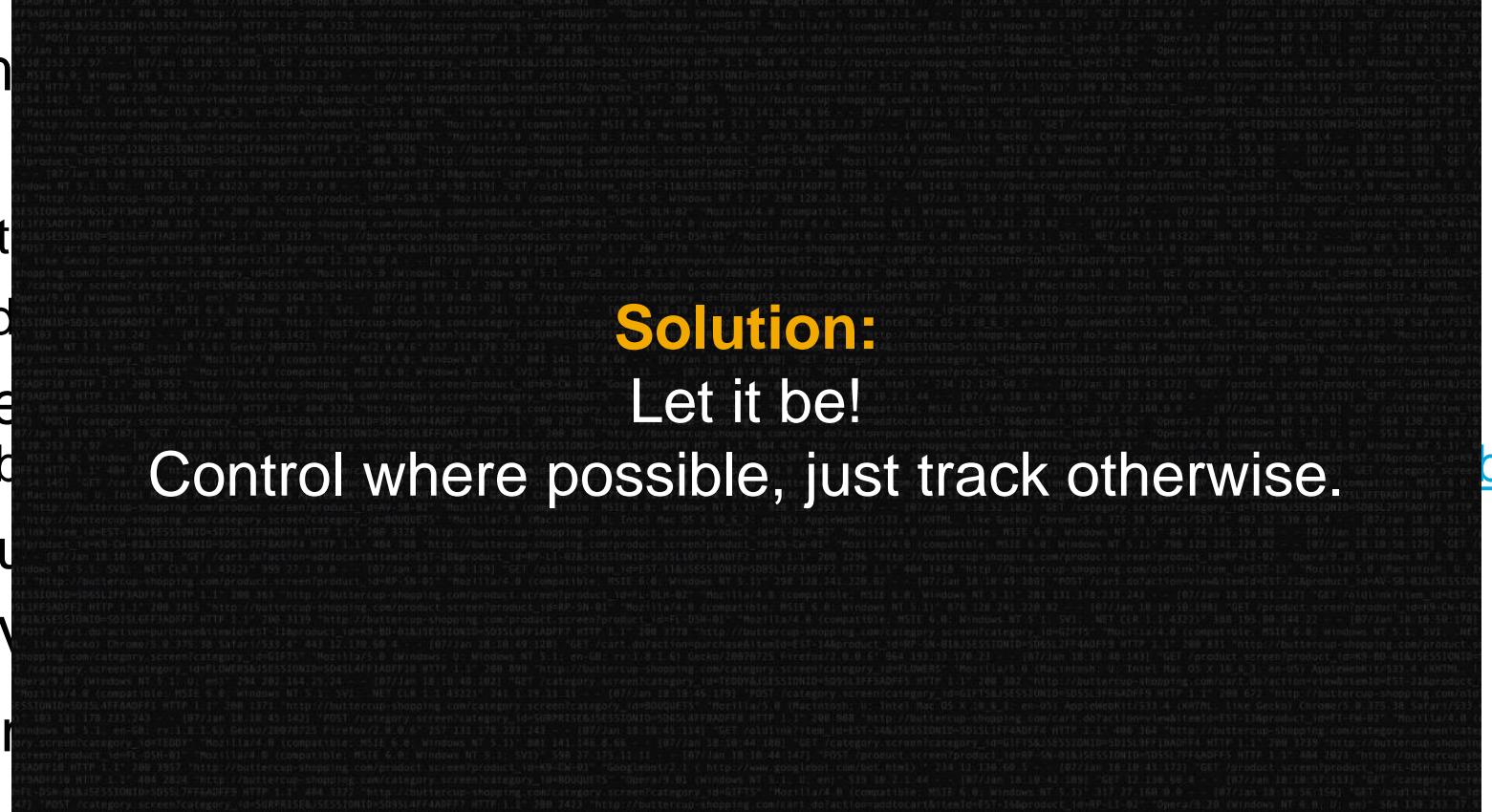
- ▶ All configs are traceable
- ▶ Multi-team collaboration
- ▶ Better code coverage
- ▶ Promote knowledge sharing
- ▶ Create a secure environment
- ▶ Off-load the system creation to the team to focus on quality, efficiency, and improvement.

Summary:

This might be too much for a small team with a single environment!

Problem: Many ways to effect change

Don't give up the flexibility of splunk's native change mechanisms

- ▶ Click in the web UI
 - ▶ Deploy something
 - deployment
 - cluster master
 - search head
 - ▶ Edit conf file
(and then probably)
 - ▶ inputlookup
 - ▶ Things in KV
 - ▶ Can you think of more?
- Solution:
Let it be!
Control where possible, just track otherwise.
[bug/refresh/](#)
- 

Just time for a quick recap

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ Tracking problem 1: precedence
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ Track all changes (inc. glass tables)
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades



138.60.4 ~ [07/Jan 18:10:57.153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=EST_6&product_name=BUTTERCUP-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.108 ~ [07/Jan 18:10:57.123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST_16&product_id=RP-LI-02" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" 468 125.17.14.108 ~ [07/Jan 18:10:56.156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&product_id=EST_6&JSESSIONID=SD10SLBFF2ADFF9" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" 468 125.17.14.108 ~ [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST_6&JSESSIONID=SD08SLBFF1ADFF4 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_6&product_id=EST_6&JSESSIONID=SD08SLBFF1ADFF4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" 468 125.17.14.108

Precedence rules



Problem: complex precedence rules

What is a rule of precedence?

/opt/splunk/etc/system/local/example.conf

/opt/splunk/etc/apps/app1/local/example.conf

Routine example.conf



=

```
[mystanza]
Option1 = A
Option2 = ??
```



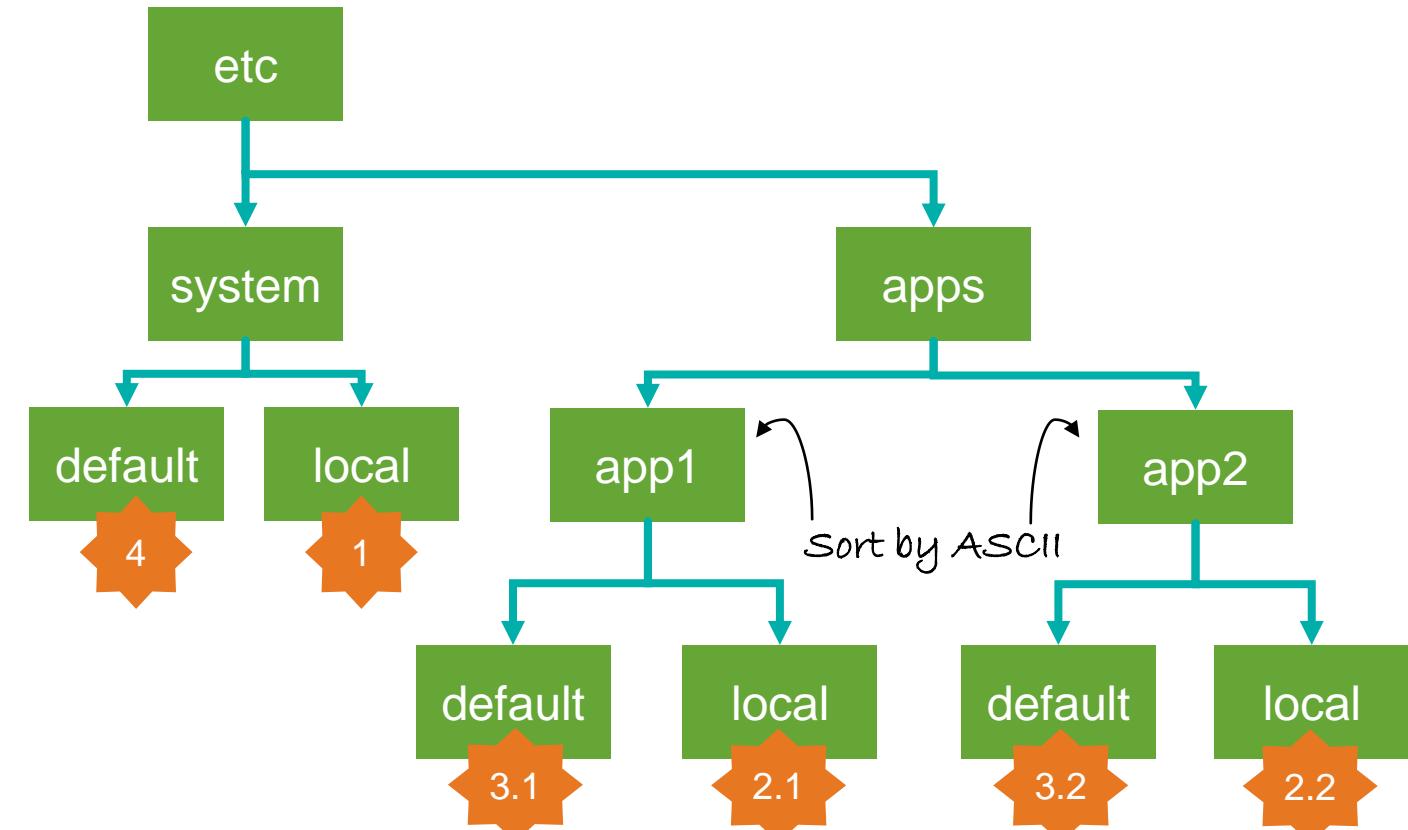
Problem: complex precedence rules

Index time processing : on indexers or forwarders

i Indexer cluster

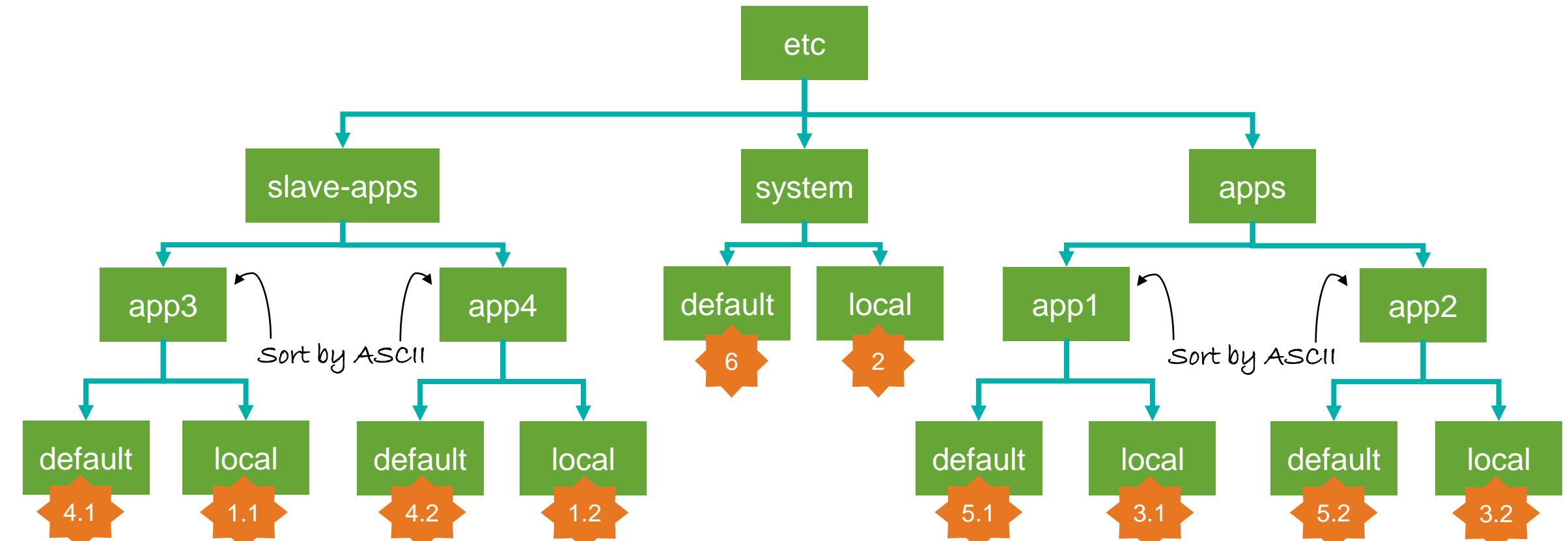
Any impact on precedence rules if you are using indexer cluster?

Answer: YES



Problem: complex precedence rules

Index time processing : on indexers



Problem: complex precedence rules

Search time processing : on search heads

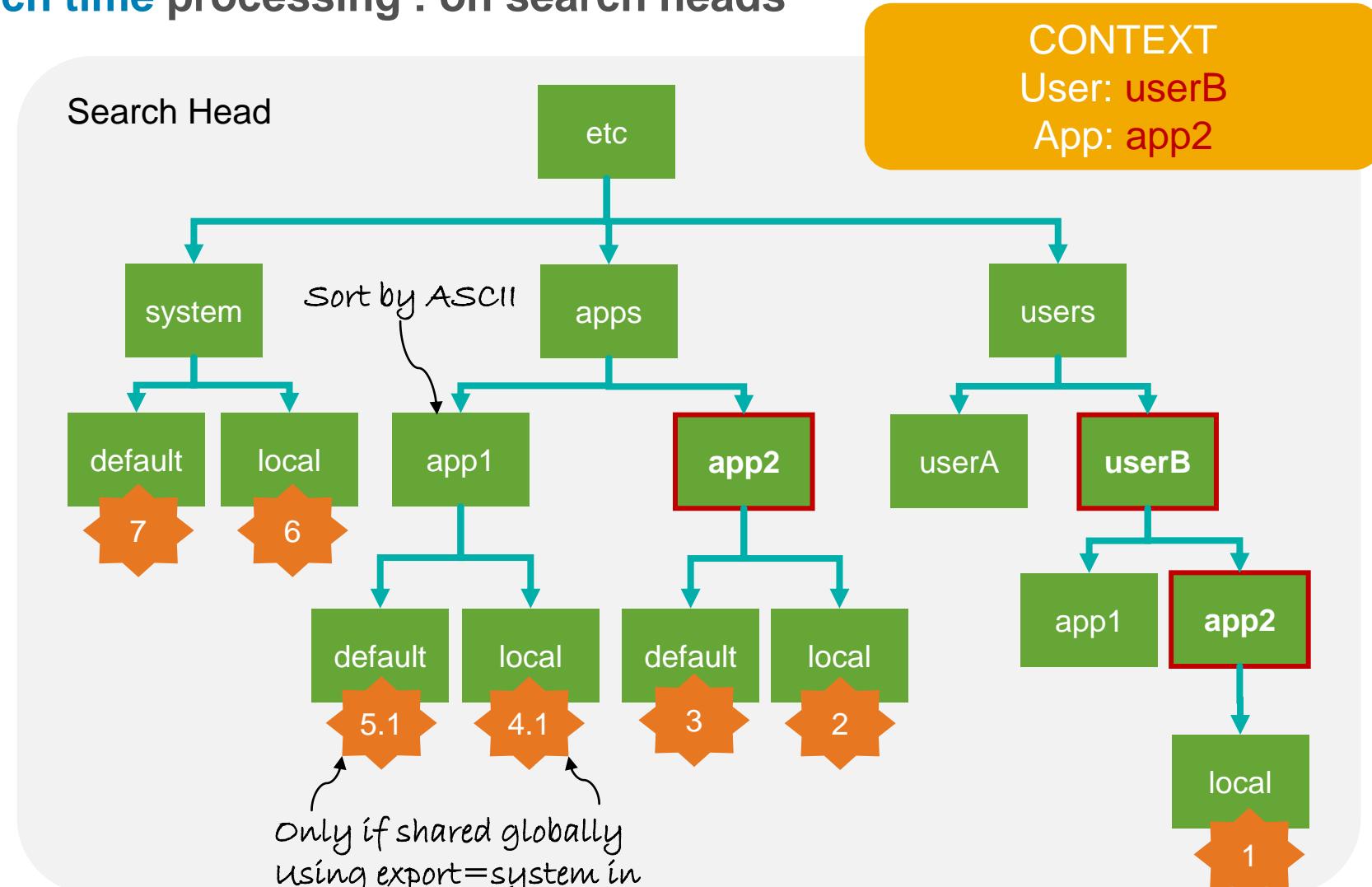
⚠ Beware of ES

“import=app1,app2,...” in metadata
overwrites the “export=system”

ⓘ Search head cluster

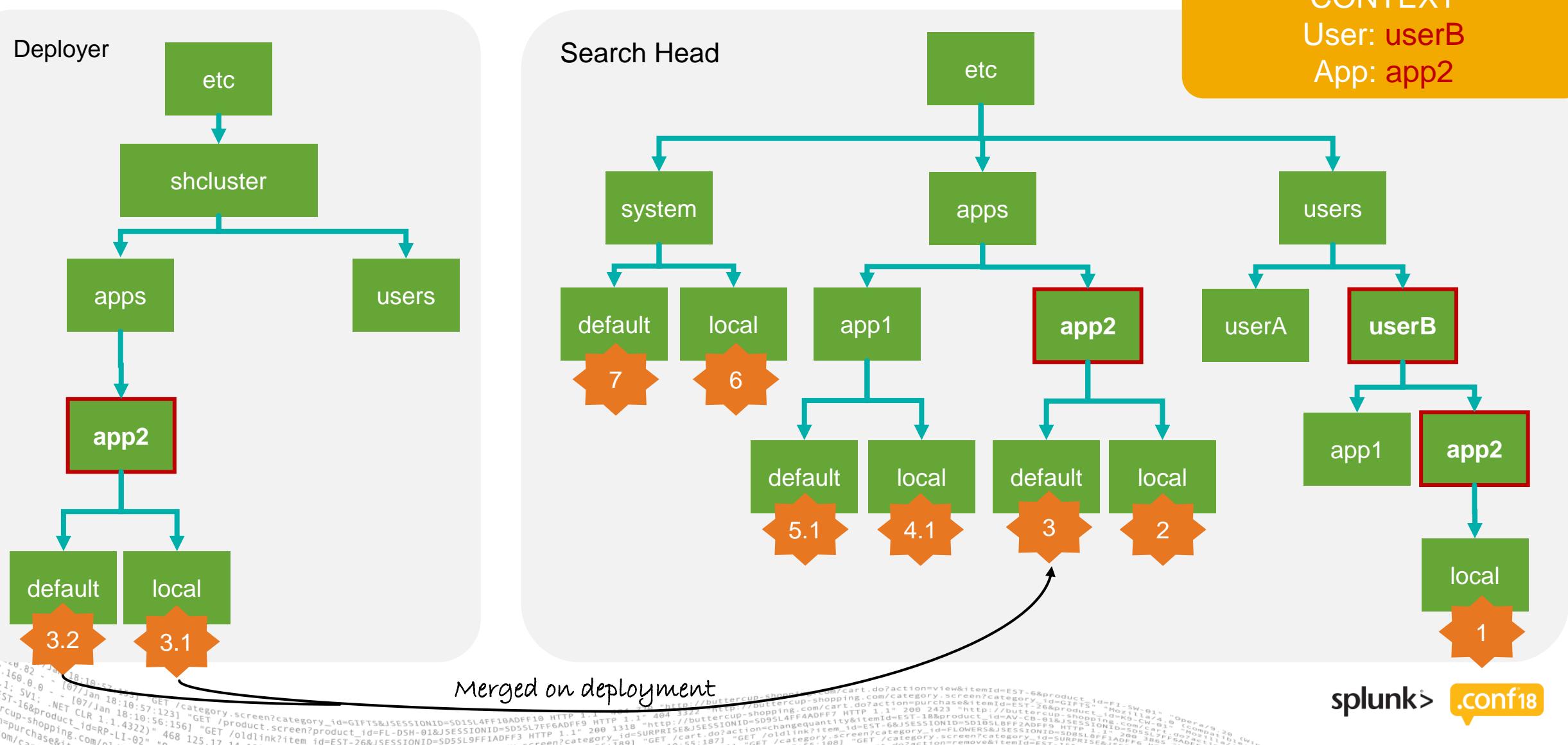
Any impact on precedence rules if
you are using search head cluster?

Answer: YES



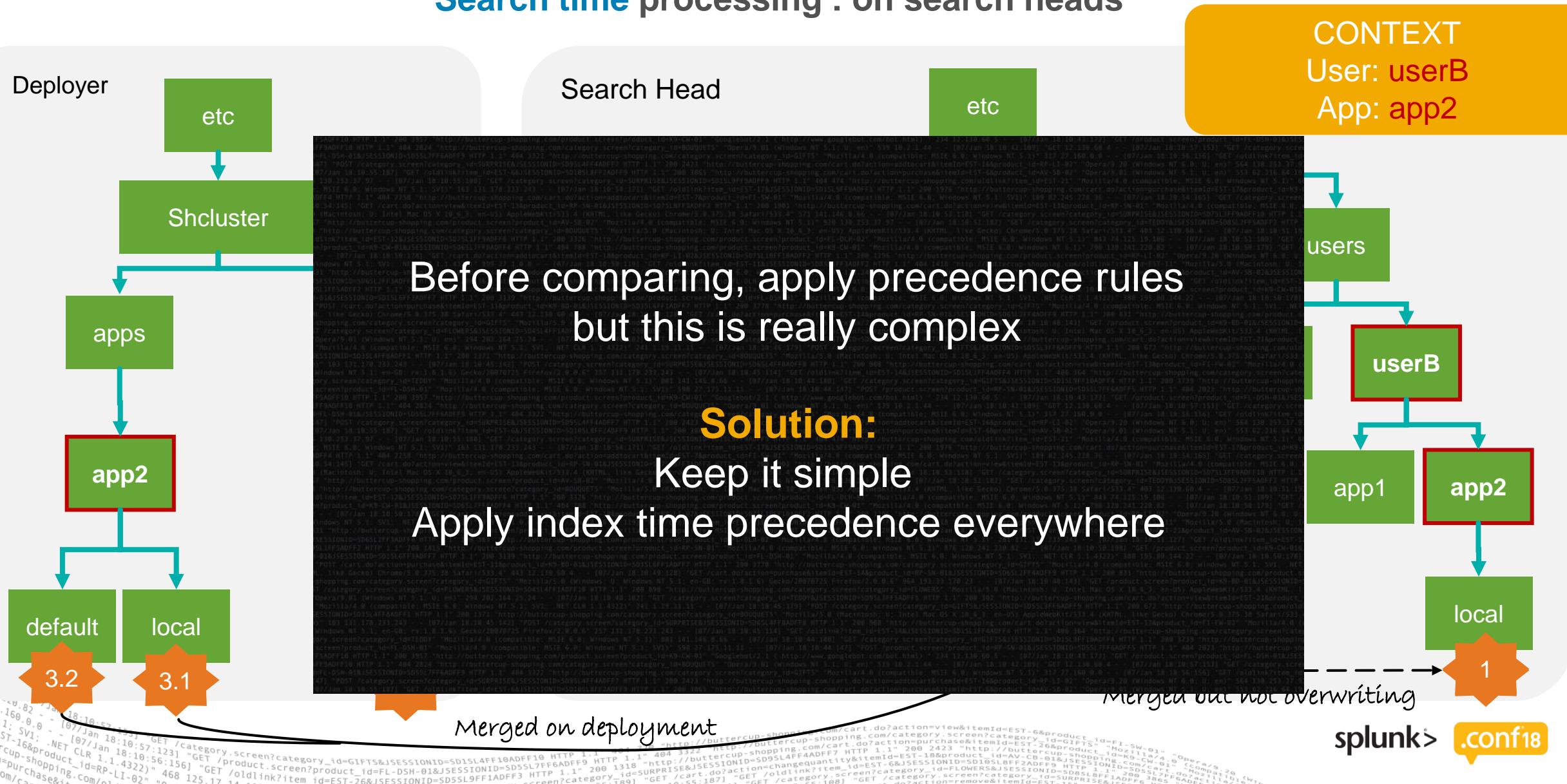
Problem: complex precedence rules

Search time processing : on search heads



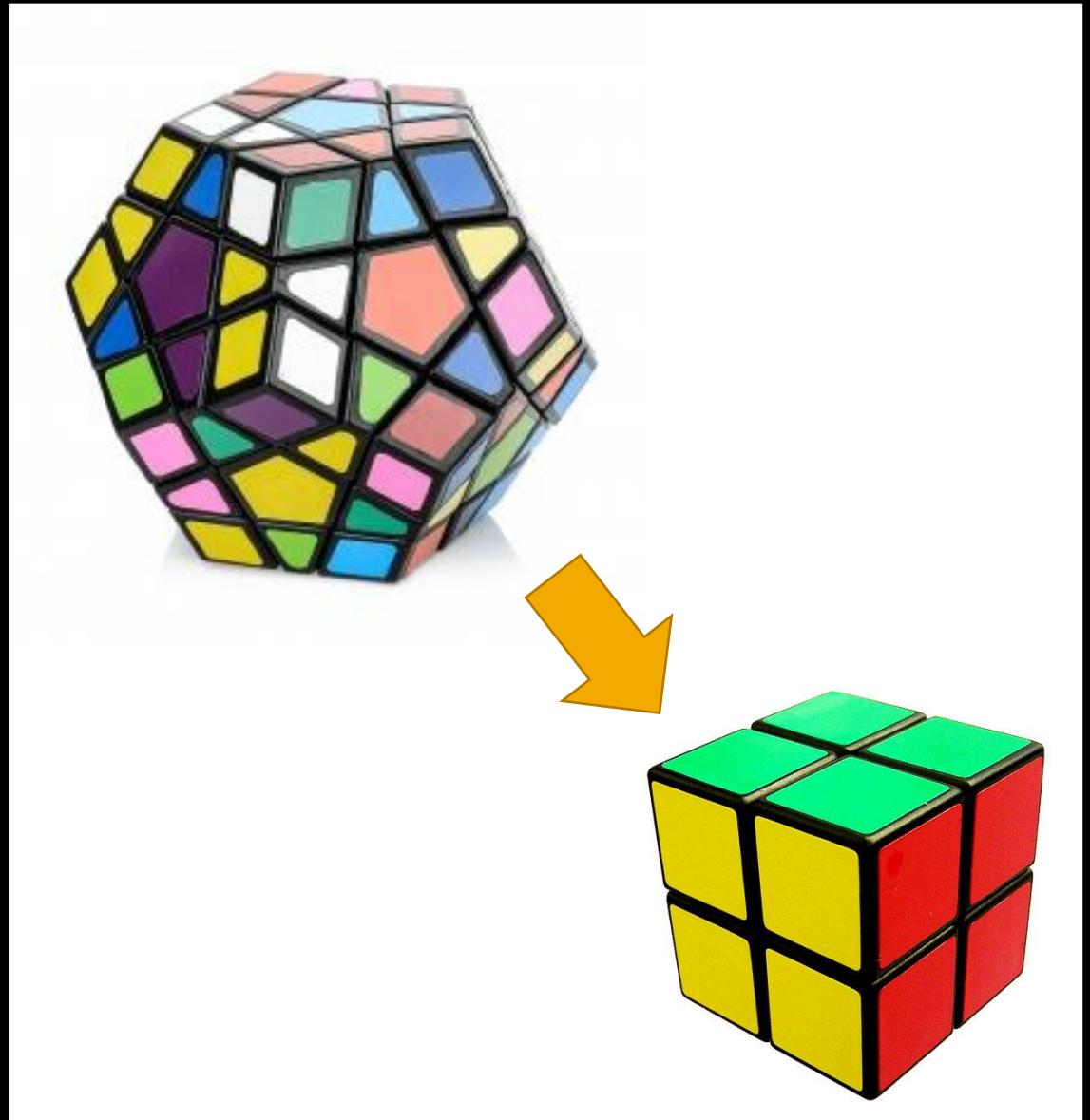
Problem: complex precedence rules

Search time processing : on search heads



Just time for a quick recap

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ **Tracking problem 1: precedence**
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ Track all changes (inc. glass tables)
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades

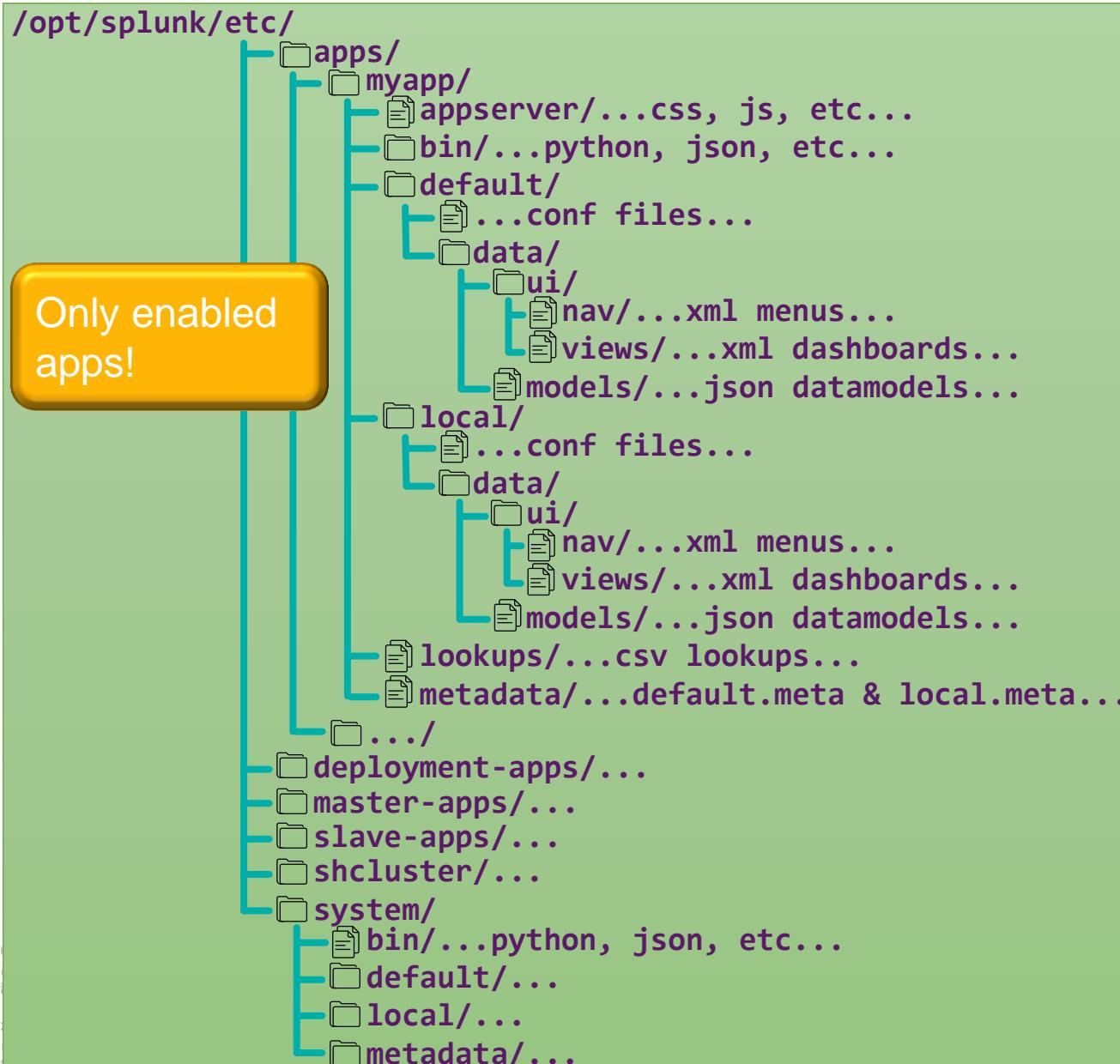


Canonical configuration

Sophisticated or over-engineered?



Splunk instance



Canonicalisation

Canonical version on disk

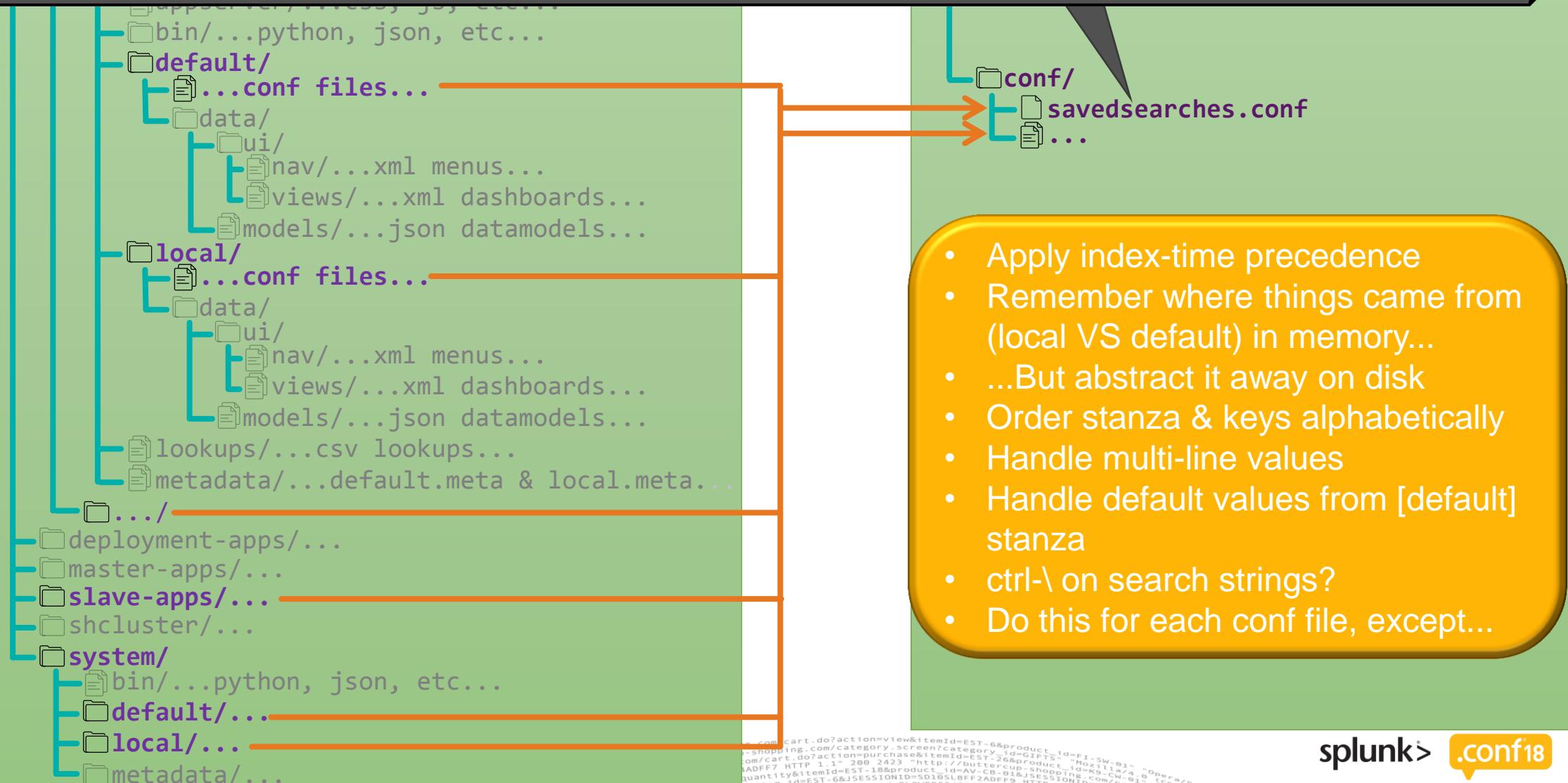
/canonical/

g.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01... "Opera/9.80 (Windows NT 5.1; U; en) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/1.0.154.38Safari/525.13" [closed]
-shopping.com/category.screen?category_id=F1-GIFTS... "Opera/9.80 (Windows NT 5.1; U; en) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/1.0.154.38Safari/525.13" [closed]
IADFFI HTTP/1.1 200 2423 "http://autoclick-shop.idsoftcw-01.com/SESSIONID=5D10SLBFF2A0DFE-HM1-1-204551-PADP-FE08899?item_id=EST-6&SESSIONID=5D10SLBFF2A0DFE-HM1-1-204551-PADP-FE08899" [closed]
category.screen?category_id=F1-GIFTS... "Opera/9.80 (Windows NT 5.1; U; en) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/1.0.154.38Safari/525.13" [closed]
category.screen?category_id=F1-GIFTS... "Opera/9.80 (Windows NT 5.1; U; en) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/1.0.154.38Safari/525.13" [closed]
category.screen?category_id=F1-GIFTS... "Opera/9.80 (Windows NT 5.1; U; en) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/1.0.154.38Safari/525.13" [closed]

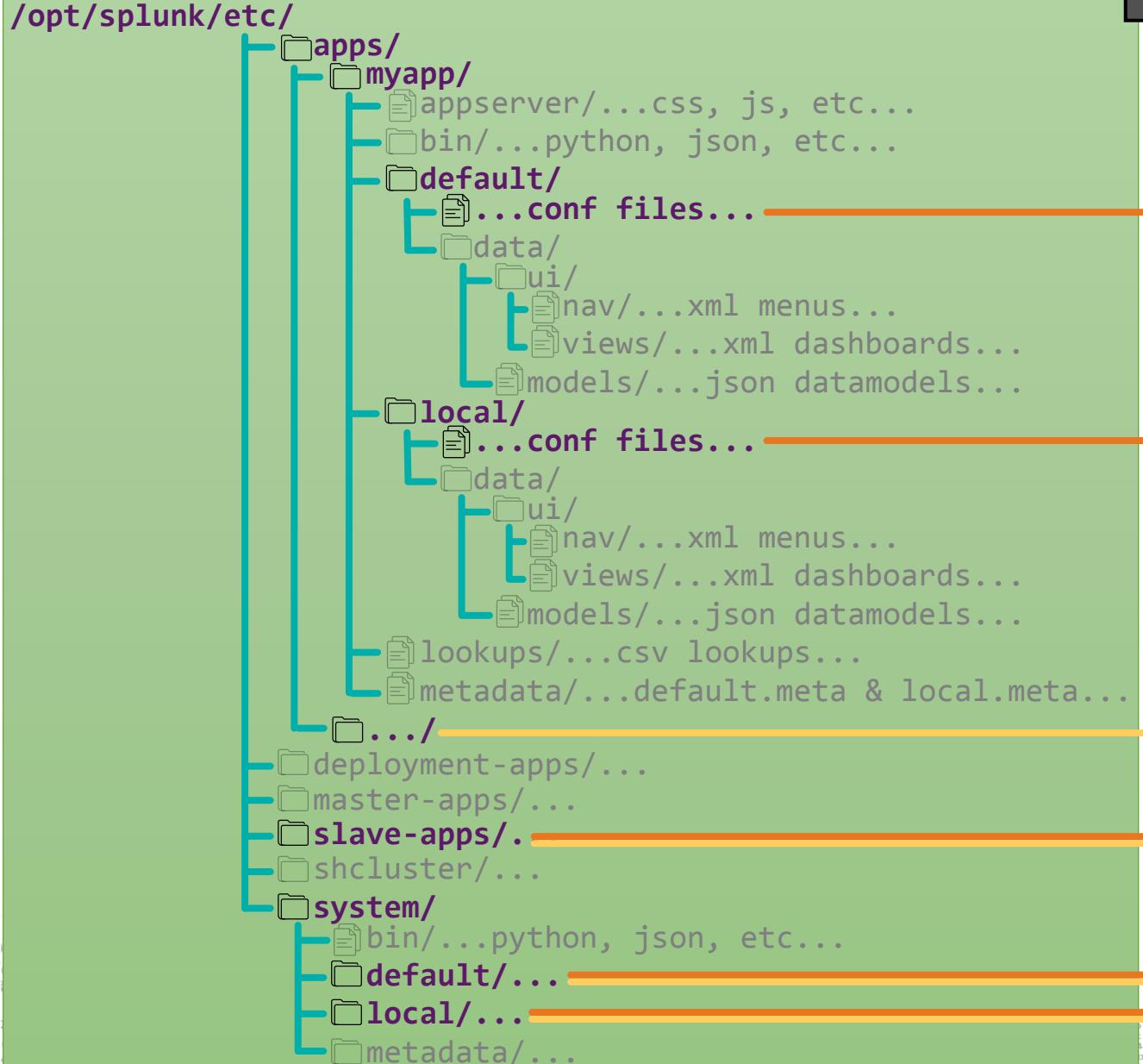
[Last known uptime by host] etc/system schedule_window = 0

[Last known uptime by host] etc/apps/nmon search = | tstats latest(...) blah blah blah
 [Last known uptime by host] etc/apps/nmon search . | stats blah blah blah
 [Last known uptime by host] etc/apps/nmon search . | eval blah blah | table blah blah

...



Splunk instance



```

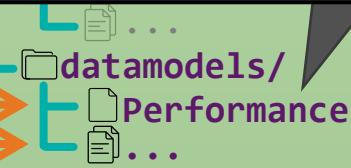
[launcher] author = Gabriel & Olivier
[ui] is_visible = 1
...
  
```

Canonical version on disk



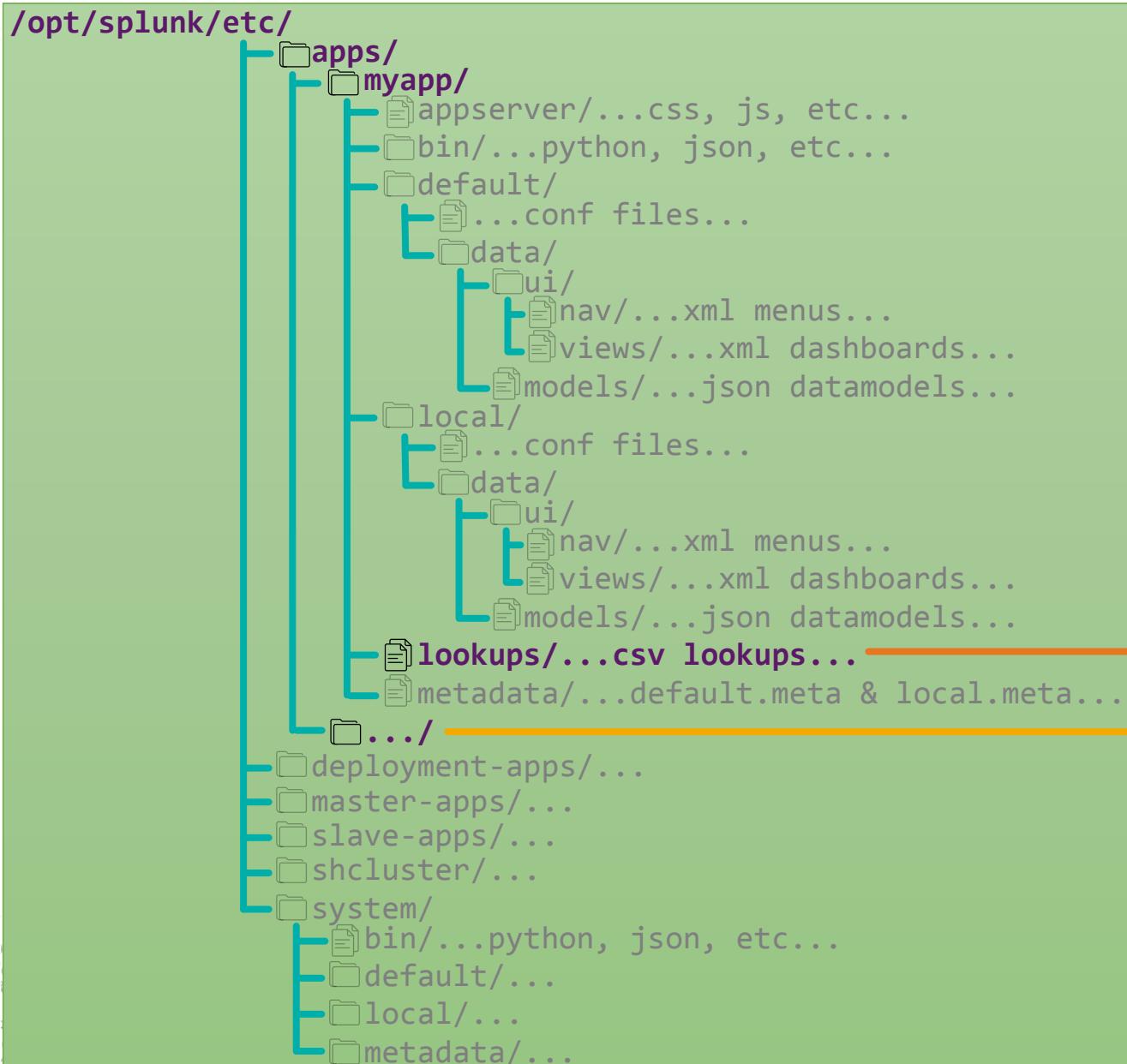
- app.conf is special!
- scope is only app-wise
- still have to apply precedence with system, but not with the other apps
- one file per app

```
Object:All_Performance - displayName: All Performance  
Object:All_Performance - parentName: BaseEvent  
Object:All_Performance - Field:dest_bunit - fieldName: dest_bunit  
Object:All_Performance - Field:dest_bunit - required: 1  
Object:All_Performance - Calculation:All_Performance_fillnull_dest - expression: if(..., ...)  
Object:CPU - parentName: All_Performance  
Object:CPU - Field:cpu_load_mhz - fieldName: cpu_load_mhz  
...  
data/  
  ui/  
    nav/...xml menus...  
    views/...xml dashboards...  
  models/...json datamodels...  
local/  
  ...conf files...  
  data/  
    ui/  
      nav/...xml menus...  
      views/...xml dashboards...  
    models/...json datamodels...  
  lookups/...csv lookups...  
  metadata/...default.meta & local.meta...  
.../  
  deployment-apps/...  
  master-apps/...  
  slave-apps/...  
  shcluster/...  
  system/  
    bin/...python, json, etc...  
    default/...  
    local/...  
    metadata/...
```



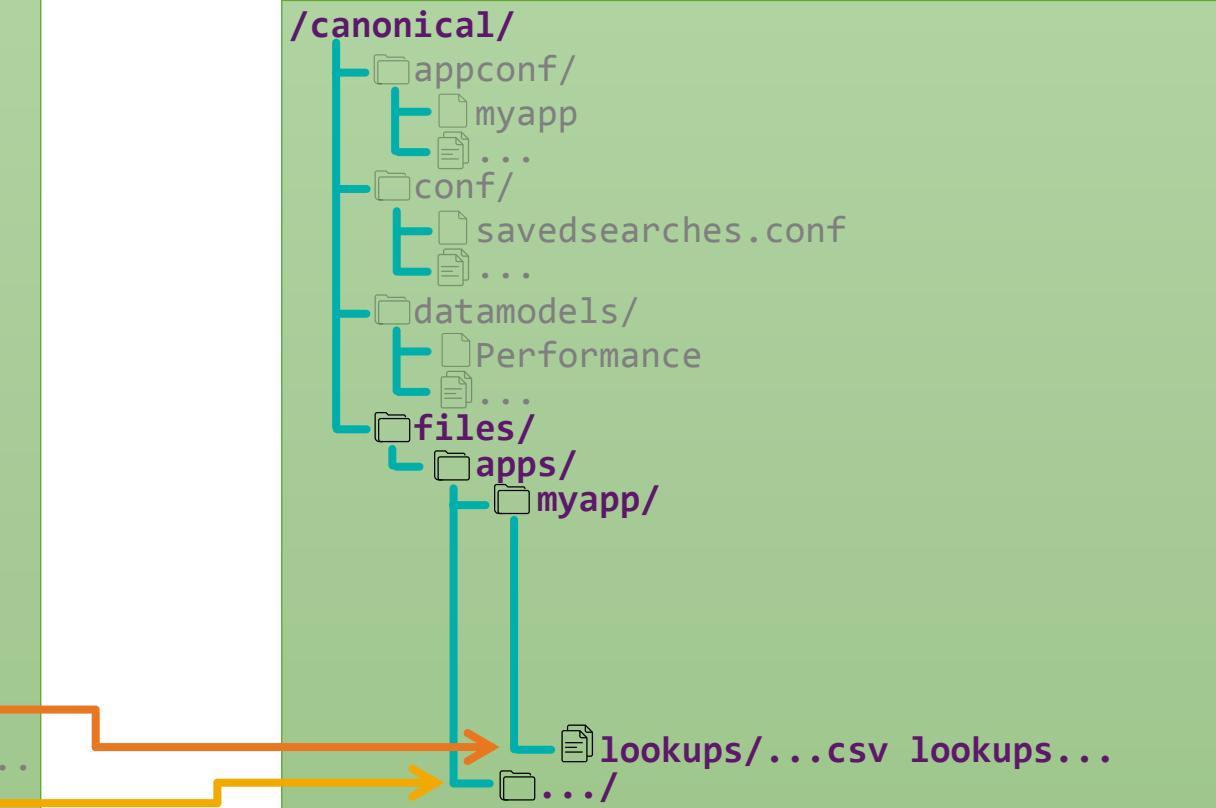
- Use precedence to find the ***one*** file that matters
- Read and parse JSON
- Beware of broken JSON!
- Rewrite:
 - remove default fields (_time source etc)
 - remove fields if present in parent/ancestor object

Splunk instance



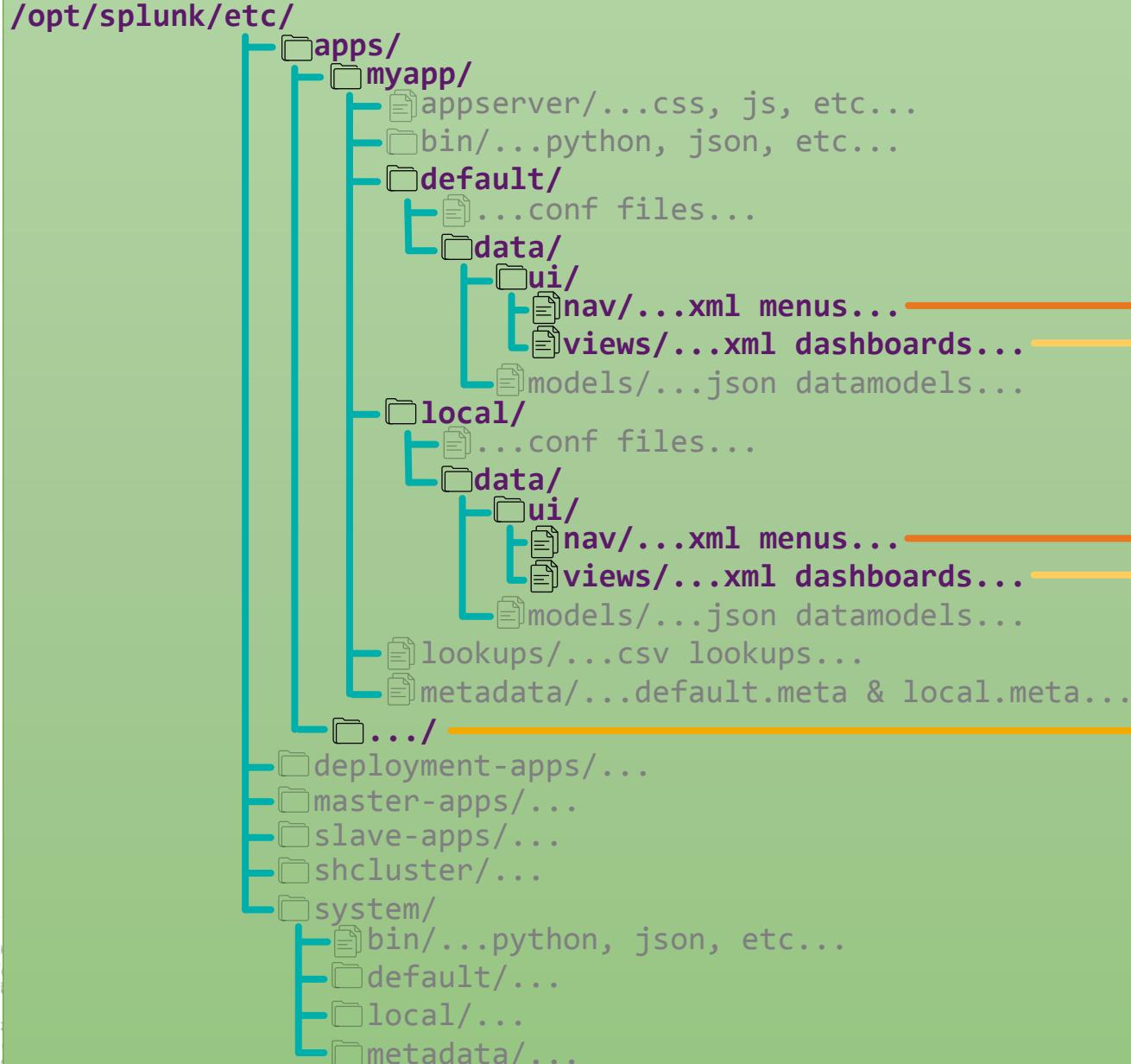
Canonicalisation – csv lookups

Canonical version on disk



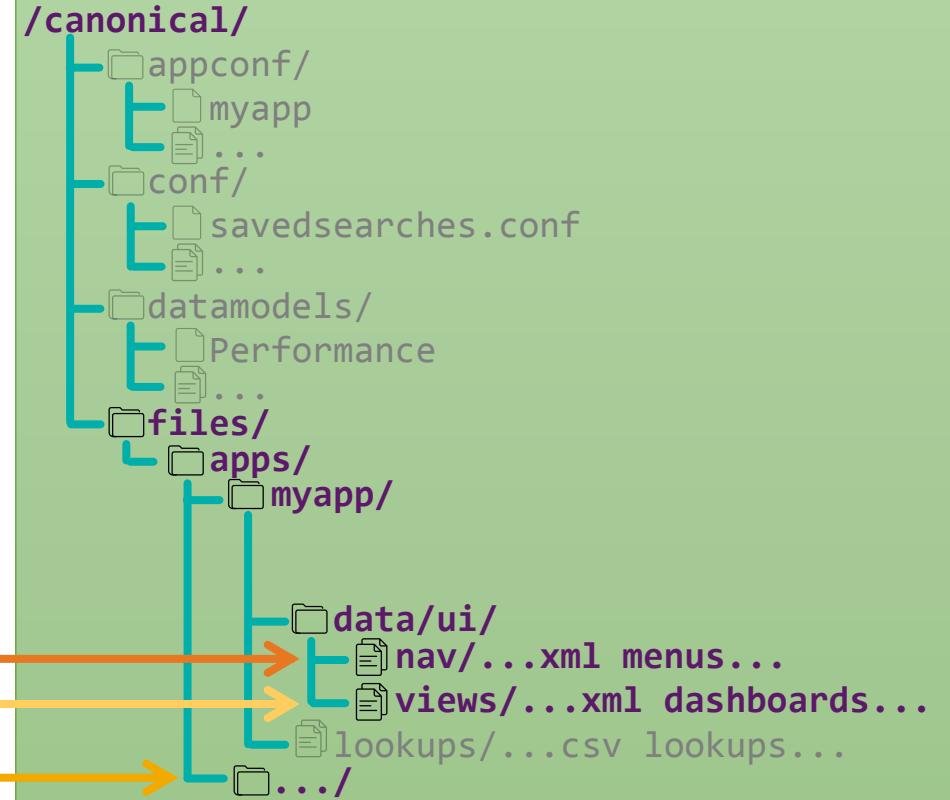
- No precedence to worry about!
- Rewrite each file:
 - order columns alphabetically
 - use library to quote consistently
 - fix any broken lookups!

Splunk instance



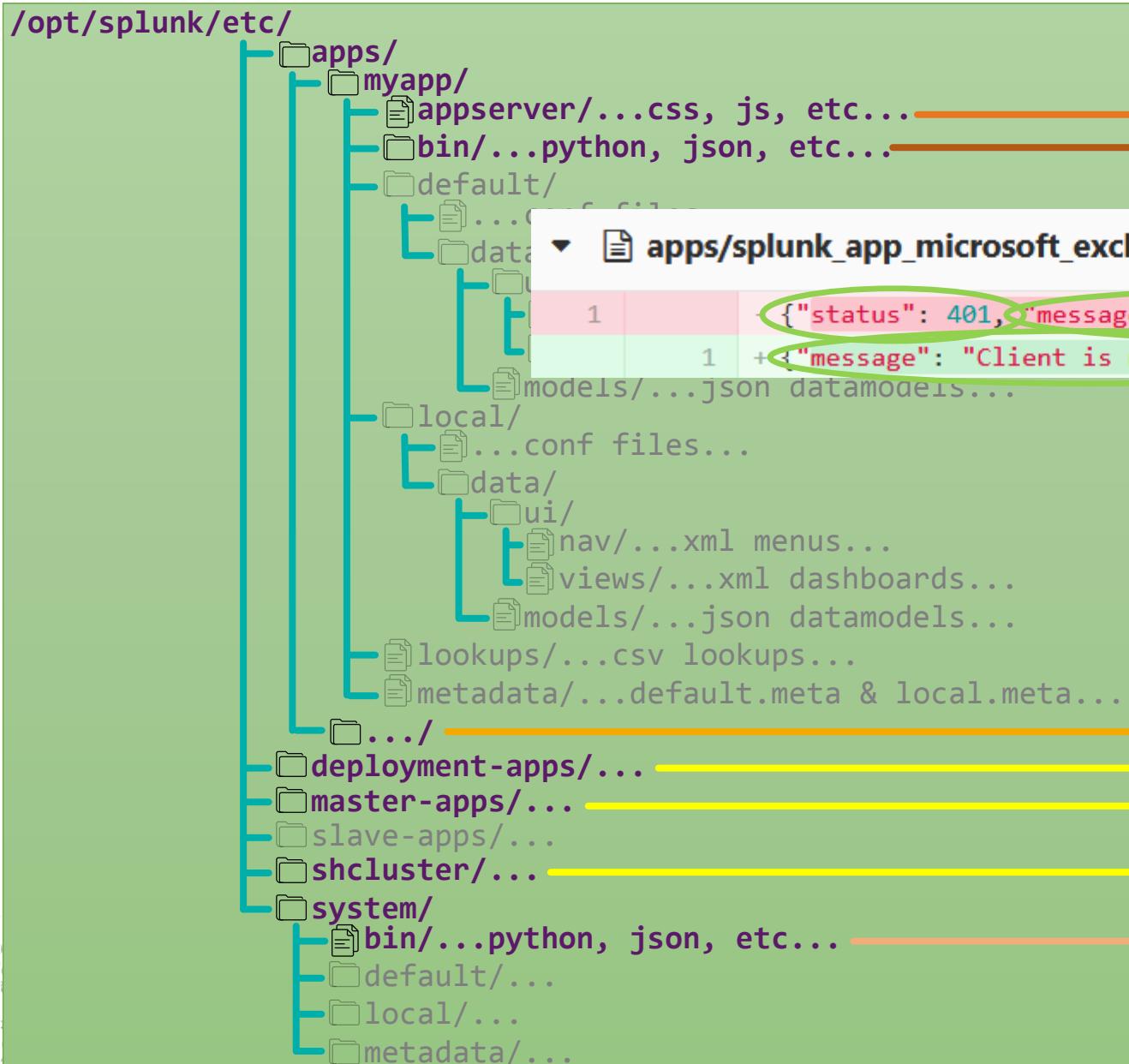
Canonicalisation – other local/default

Canonical version on disk



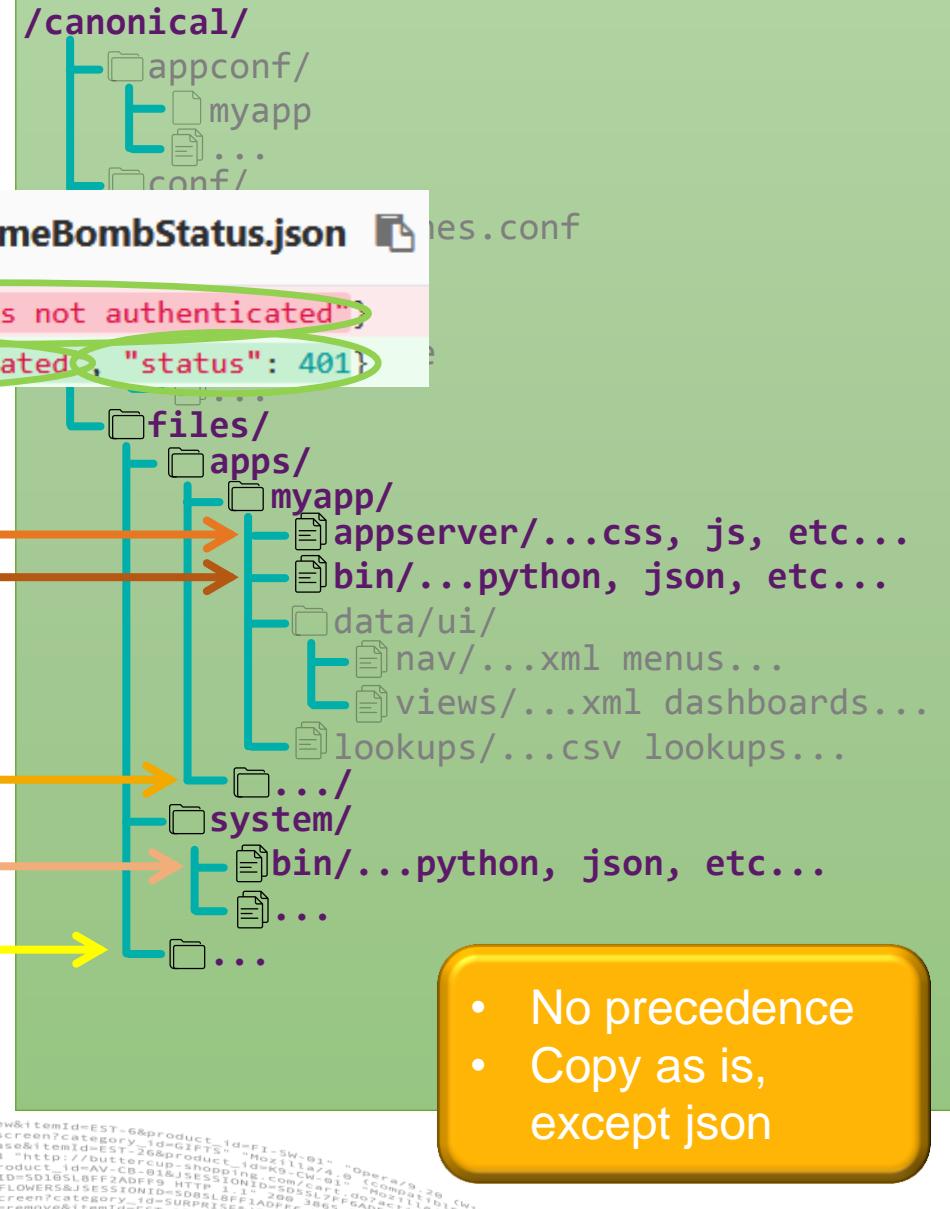
- Take local file if present, otherwise take default file
- Just take the file as it is!

Splunk instance



Canonicalisation – anything else

Canonical version on disk



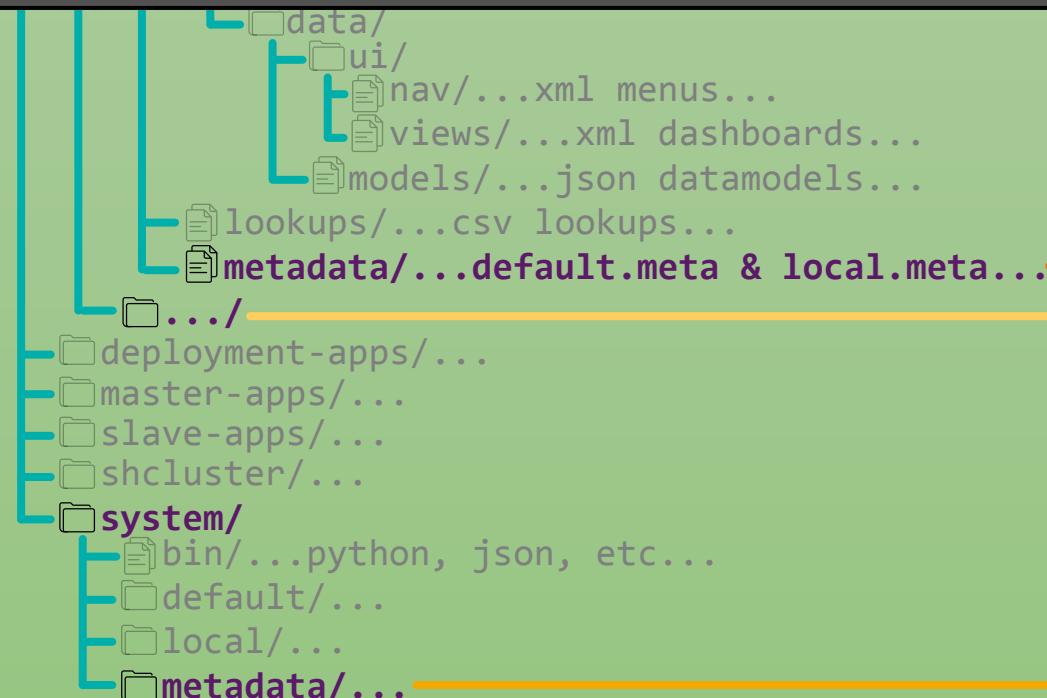
Splunk instance

Canonicalisation – metadata



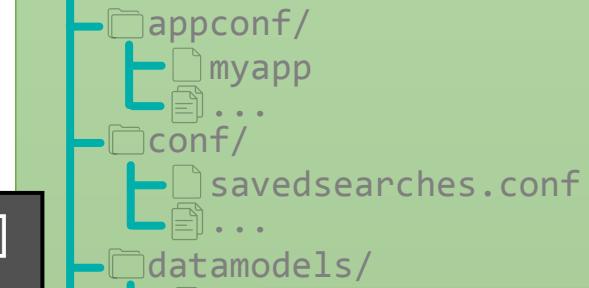
```
[eventtypes/HighRisk] access = read: [*], write: [admin]
[eventtypes/HighRisk] export = system
[eventtypes/HighRisk] owner = Gabriel
...

```



Canonical version on disk

/canonical/



- Can be important!
- Apply precedence between default.meta and local.meta
- Keep each app and system separate (or not)
- Ignore modtime, too noisy!
- Ignore version (noisy)

Re-inventing btool

but better!

- ▶ DIGRESSION: When you've re-invented btool you can do some pretty cool searching and filtering!
- ▶ E.g. I want the cron schedule and search string of every enabled correlation searches that use the Web data model
 - for each saved search:
 - is it a correlation search?
 - is it not disabled?
 - does the 'search' key contain "Web."?
 - if yes to all, display the stanza name, cron_schedule and search string



Just time for a quick recap

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ Tracking problem 1: precedence
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ Track all changes (inc. glass tables)
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades



Diff explosions

A.k.a. the diff butterfly effect



explosion 1: conf stanza

Correlation Search

Search Name *

Completely Inactive Account

Application Context *

SA-AccessProtection

UI Dispatch Context *

None

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description

Accounts that are no longer used.

Describes what kind of issues this search is intended to detect.

Mode

Guided

Manual

Search *

```
| inputlookup append=T access_tracker | eval user=lower(user) | sort -userLastTime | dedup user where ((now() - userLastTime) / 86400) > 0
```

Time Range

Earliest Time

Set a time range of events to search. Type an earliest time using relative time modifiers.

Latest Time

Type a latest time using relative time modifiers.

Cron Schedule *

40 ** 6

Enter a cron-style schedule. For example */5 * * * *

(every 5 minutes), or 0 0 1 * * (every day at 0 AM)

explosion 1: conf stanza

etc/apps/SA-AccessProtection/local/savedsearches.conf

```

1 [Access - Completely Inactive Account - Rule]
2 - action.nbtstat.param.verbose = 0
3 - action.nslookup.param.verbose = 0
4 - action.ping.param.verbose = 0
5 - description = Accounts that are no longer used.
6 - dispatch.rt_backfill = 1
7 -
8 [Access - Insecure Or Cleartext Authentication - Rule]
9 action.customsearchbuilder.enabled = true
10 action.nbtstat.param.verbose = 0
...
92 relation = greater than
93 schedule_window = auto
94 search = | tstats allow_old_summaries=true summariesonly=t values(All_Sessions.src_ip) AS src_ip count from
datamodel=Network_Sessions where nodename=All_Sessions.VPN All_Sessions.action=failure by
All_sessions.thales_customer All_Sessions.user | where count>19 |`drop_dm_object_name(All Sessions)
88 +
89 + [Access - Completely Inactive Account - Rule]
90 + action.customsearchbuilder.enabled = raise
91 + action.nbtstat.param.verbose = 0
92 + action.nslookup.param.verbose = 0
93 + action.ping.param.verbose = 0
94 + cron_schedule = 1 0 * * *
95 - description = Accounts that are no longer used.
96 + dispatch.rt_backfill = 1
97 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showBackwards = 0
98 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLabels = 1
99 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLegend = 1
100 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showSelf = 0
101 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showTooltip = 1
102 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.styleBackwards = 0
103 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.useColors = 1

```

explosion 1: conf stanza

```

...
5710 5710 @@ -5710,6 +5710,7 @@ vsid =
5711 5711     action.correlationsearch = 0
5712 5712     action.correlationsearch.enabled = 1
5713 5713     action.correlationsearch label = Completely Inactive Account
+ action.customsearchbuilder.enabled = false

```

```

5714 5714     action.email = 1
5715 5715     action.email.format = csv
5716 5716     action.email.inline = 1
...
5767 5768     auto_summarize.suspend_period = 24h
5768 5769     auto_summarize.timespan =
5769 5770     counttype = number of events

```

```

5770 5770     - cron_schedule = 3 0 * * 6
5771 5771     + cron_schedule = 4 0 * * 6
5772 5772     description = Accounts that are no longer used.
5773 5773     disabled = 0
5774 5774     dispatch.auto_cancel = 0
...
5862 5863     display.visualizations.custom.sankey_diagram_app.sankey_diagram.colorMode = cate
5863 5864     display.visualizations.custom.sankey_diagram_app.sankey_diagram.maxColor = #3fc77a
5864 5865     display.visualizations.custom.sankey_diagram_app.sankey_diagram.minColor = #d93f3c

```

```

5865 5865     - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showBackwards = false
5866 5866     - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLabels = true
5867 5867     - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLegend = true
5868 5868     - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showSelf = false
5869 5869     - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showTooltip = true
5870 5870     - display.visualizations.custom.sankey_diagram_app.sankey_diagram.styleBackwards = false
5871 5871     - display.visualizations.custom.sankey_diagram_app.sankey_diagram.useColors = true

```

```

5866 5866     + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showBackwards = 0
5867 5867     + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLabels = 1
5868 5868     + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLegend = 1
5869 5869     + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showSelf = 0
5870 5870     + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showTooltip = 1
5871 5871     + display.visualizations.custom.sankey_diagram_app.sankey_diagram.styleBackwards = 0
5872 5872     + display.visualizations.custom.sankey_diagram_app.sankey_diagram.useColors = 1

```

> splunk btool savedsearches list



which search?

... ... @@ -5684,6 +5684,7 @@

5684 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.correiationsearch.label =

5685 [Access - Completely Inactive Account - Rule]

5686 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.correiationsearch.enabled = 1

5687 + [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.customsearchbuilder.enabled = false

5688 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.email = 1

5689 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.email.format = csv

5690 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.email.inline = 1

... ... @@ -5741,7 +5742,7 @@

5741 [Access - Completely Inactive Account - Rule] etc/system auto_summarize.suspend_period = 24h

5742 [Access - Completely Inactive Account - Rule] etc/system auto_summarize.timespan =

5743 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection counttype = number of events

5744 - [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection cron_schedule = 3 0 * * 6

5745 + [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection cron_schedule = 4 0 * * 6

5746 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection description = Accounts that are no longer used.

5747 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection disabled = 0

5748 [Access - Completely Inactive Account - Rule] etc/system dispatch.auto_cancel = 0

... ... @@ -5836,13 +5837,13 @@

5836 [Access - Completely Inactive Account - Rule] etc/apps/sankey_diagram_app

display.visualizations.custom.sankey_diagram_app.sankey_diagram.maxColor = #3fc77a

5837 [Access - Completely Inactive Account - Rule] etc/apps/sankey_diagram_app

display.visualizations.custom.sankey_diagram_app.sankey_diagram.minColor = #d93f3c

5838 [Access - Completely Inactive Account - Rule] etc/apps/sankey_diagram_app

display.visualizations.custom.sankey_diagram_app.sankey_diagram.numOfBins = 6

5839 - [Access - Completely Inactive Account - Rule] etc/system

display.visualizations.custom.sankey_diagram_app.sankey_diagram.showBackwards = false

- [Access - Completely Inactive Account - Rule] etc/system

display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLabels = true

- [Access - Completely Inactive Account - Rule] etc/system

display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLegend = true

- [Access - Completely Inactive Account - Rule] etc/system

display.visualizations.custom.sankey_diagram_app.sankey_diagram.showSelf = false

- [Access - Completely Inactive Account - Rule] etc/system

display.visualizations.custom.sankey_diagram_app.sankey_diagram.showTooltip = true

- [Access - Completely Inactive Account - Rule] etc/system

display.visualizations.custom.sankey_diagram_app.sankey_diagram.styleBackwards = false

- [Access - Completely Inactive Account - Rule] etc/system

display.visualizations.custom.sankey_diagram_app.sankey_diagram.useColors = true

5840 + [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection

display.visualizations.custom.sankey_diagram_app.sankey_diagram.showBackwards = 0

explosion 1: conf stanza



EST-68product_id=F1-SW-01...
=EST-26&product_id=d942911a/4@0...
butercup-showtime.com-w-01...
AV-COM-SESSIONID=00000000000000000000000000000000
SESSIONID=5D8SLBPF-3865-PADP-FE
group=SURPRISE&PADP-FE
enid=EST-26&product_id=d942911a/4@0...
butercup-showtime.com-w-01...
AV-COM-SESSIONID=00000000000000000000000000000000

Explosion 2: Data model definition

Performance

Performance

[All Data Models](#)

Datasets [Add Dataset ▾](#) All Performance All_Performance [Rename](#) [Delete](#)

EVENTS

All Performance

- CPU
- Facilities
- Memory
- Storage
- Network
- OS
 - Time Synchronization
 - System Uptime

CONSTRAINTS

```
(`cim_Performance_indexes`) tag=performance (tag=cpu OR tag=facilities OR tag=memory OR tag=storage OR tag=network OR (tag=os ((tag=time tag=synchronize) OR tag=uptime)))
```

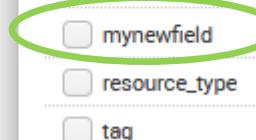
Bulk Edit ▾ [Add Field ▾](#)

INHERITED

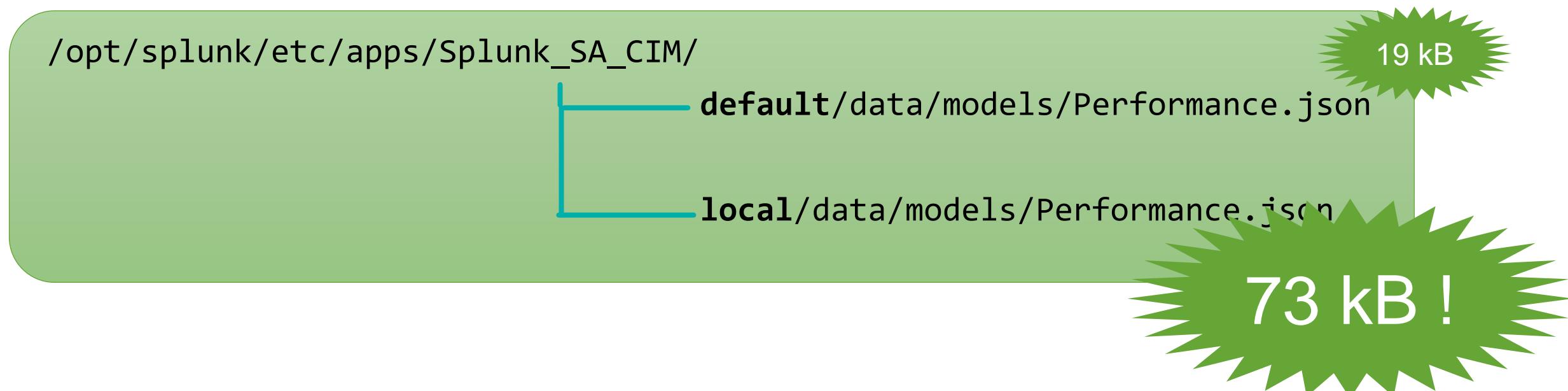
	Type	
_time	Time	
<input type="checkbox"/> host	String	Override
<input type="checkbox"/> source	String	Override
<input type="checkbox"/> sourcetype	String	Override

EXTRACTED

	Type	
<input type="checkbox"/> dest_bunit	String	Edit
<input type="checkbox"/> dest_category	String	Edit
<input type="checkbox"/> dest_priority	String	Edit
<input type="checkbox"/> dest_should_timesync	Boolean	Edit
<input type="checkbox"/> dest_should_update	Boolean	Edit
<input type="checkbox"/> hypervisor_id	String	Edit
<input checked="" type="checkbox"/> mynewfield	String	Edit
<input type="checkbox"/> resource_type	String	Edit
<input type="checkbox"/> tag	String	Edit



Explosion 2: Data model definition



```

138.60.4.1 - - [07/Jan/18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=putInSession&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /oldlink?item_id=EST_26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST_18&productId=AU-CUP-SHOPPING.COM-SWT-DESKTOP-0551-PAD-PRO-102&product_id=EST_16&product_id=RPLI-02" "GET /oldlink?item_id=EST_6&JSESSIONID=SD15SLBFF2ADFF1 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST_18&productId=AU-CUP-SHOPPING.COM-SWT-DESKTOP-0551-PAD-PRO-102&product_id=EST_16&product_id=RPLI-02" "GET /oldlink?item_id=EST_6&JSESSIONID=SD15SLBFF2ADFF1 HTTP/1.1" 200 3865 "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=putInSession&itemId=EST_26&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "GET /oldlink?item_id=EST_26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST_18&productId=AU-CUP-SHOPPING.COM-SWT-DESKTOP-0551-PAD-PRO-102&product_id=EST_16&product_id=RPLI-02" "GET /oldlink?item_id=EST_6&JSESSIONID=SD15SLBFF2ADFF1 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST_18&productId=AU-CUP-SHOPPING.COM-SWT-DESKTOP-0551-PAD-PRO-102&product_id=EST_16&product_id=RPLI-02" "GET /oldlink?item_id=EST_6&JSESSIONID=SD15SLBFF2ADFF1 HTTP/1.1" 200 3865
    
```

Explosion 2: Data model definition

```
79      "required": false,  
80      "multivalue": false,  
81      "hidden": false  
82    },  
83    {  
84      "comment": {"description": "This automatically  
generated field is used to access tags from within data models. Add-on builders do not need to populate  
it.", "ta_relevant": false},  
85      "fieldName": "tag",  
86      "displayName": "tag",  
87      "type": "string",  
88      "fieldSearch": "",  
89      "required": false,  
90      "multivalue": true,  
91      "hidden": false  
92    },  
93      "required": false,  
94      "multivalue": false,  
95      "hidden": false,  
96      "editable": true,  
97      "displayName": "resource_type",  
98      "comment": ""  
99    },  
100   {  
101      "fieldName": "tag",  
102      "owner": "All_Performance",  
103      "type": "string",  
104      "fieldSearch": "",  
105      "required": false,  
106      "multivalue": true,  
107      "hidden": false,  
108      "editable": true,  
109      "displayName": "tag",  
110      "comment": ""  
111    },  
112    {  
113      "fieldName": "mynewfield",  
114      "owner": "All_Performance",  
115      "type": "string",  
116      "fieldSearch": "",  
117      "required": false,  
118      "multivalue": false,  
119      "hidden": false,  
120      "editable": true,  
121      "displayName": "mynewfield",  
122      "comment": ""  
123    },  
124    {  
125      "fieldName": "_time",  
126      "owner": "BaseEvent",  
127      "type": "timestamp",  
128      "fieldSearch": "",  
129      "required": false,  
130      "multivalue": false,  
131      "hidden": false,  
132      "editable": true,  
133      "displayName": "_time",  
134      "comment": ""  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
999  
1000
```

Explosion 2: Data model definition

Performance

Performance

< All Data Models

Edit Download Pivot Documentation

Datasets

Add Dataset

Rename Delete

EVENTS

All Performance

- CPU
- Facilities
- Memory
- Storage
- Network
- OS
 - Time Synchronization
 - System Uptime

constraint Edit

Add Field

Override

Override

Override

Edit

dest_category String Edit

dest_priority String Edit

dest_should_timesync Boolean Edit

dest_should_update Boolean Edit

hypervisor_id String Edit

mynewfield String Edit

resource_type String Edit

tag String Edit



.conf18

~~Explosion~~ 2: Data model definition

File datamodels/Performance More		
...	...	@@ -42,6 +42,12 @@ DM:Performance - Object:All_Performance - Field:hypervisor_id - type: string
42	42	DM:Performance - Object:All_Performance - Field:hypervisor_id - required: 1
43	43	DM:Performance - Object:All_Performance - Field:hypervisor_id - hidden: 1
44	44	DM:Performance - Object:All_Performance - Field:hypervisor_id - multivalue: 1
	45	+ DM:Performance - Object:All_Performance - Field:mynewfield - fieldName: mynewfield
	46	+ DM:Performance - Object:All_Performance - Field:mynewfield - displayName: mynewfield
	47	+ DM:Performance - Object:All_Performance - Field:mynewfield - type: string
	48	+ DM:Performance - Object:All_Performance - Field:mynewfield - required: 1
	49	+ DM:Performance - Object:All_Performance - Field:mynewfield - hidden: 1
	50	+ DM:Performance - Object:All_Performance - Field:mynewfield - multivalue: 1
45	51	DM:Performance - Object:All_Performance - Field:resource_type - fieldName: resource_type
46	52	DM:Performance - Object:All_Performance - Field:resource_type - displayName: resource_type
47	53	DM:Performance - Object:All_Performance - Field:resource_type - type: string
...	...	

COOL

130,60,4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_68&product_id=F1-SW-01" "Opera/9.20 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=updateSession&itemId=EST_26&product_id=AUTOCUP-SHOWCASE-LIGHT-CW-01" "Compatilis (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST_18&productId=AUTOCUP-SHOWCASE-LIGHT-CW-01" "Compatilis (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST_68&JSESSIONID=SD10SLBFF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=retrieveSession" "SurprisePad PRO" [07/Jan 18:10:55:188] "GET /category.screen?category_id=SURPRISEPAD-PRO&JSESSIONID=SD08SLBFF3ADFF6 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_70&product_id=FP-10" "SurprisePad PRO" [07/Jan 18:10:55:189] "GET /category.screen?category_id=SURPRISEPAD-PRO&JSESSIONID=SD08SLBFF3ADFF6 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=retrieveSession" "SurprisePad PRO" [07/Jan 18:10:55:188] "GET /category.screen?category_id=SURPRISEPAD-PRO&JSESSIONID=SD08SLBFF3ADFF6 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_70&product_id=FP-10" "SurprisePad PRO"

Explosion 3: csv lookup

	just_for_fun.csv
1	zzz,aaa
2	hello,bonjour
3	hi,au revoir
4	hello world,bonjour tout le monde
5	hello world!,bonjour tout le monde!

A screenshot of the Splunk interface showing a search results page. A green oval highlights the search command in the search bar:

```
| inputlookup just_for_fun.csv
| eval zzz=replace(zzz,"hi","goodbye")
| outputlookup just_for_fun.csv
```

The search results table shows the following data:

aaa	zzz
bonjour	hello
au revoir	goodbye
bonjour tout le monde	hello world
bonjour tout le monde!	hello world!

Explosion 3: csv lookup

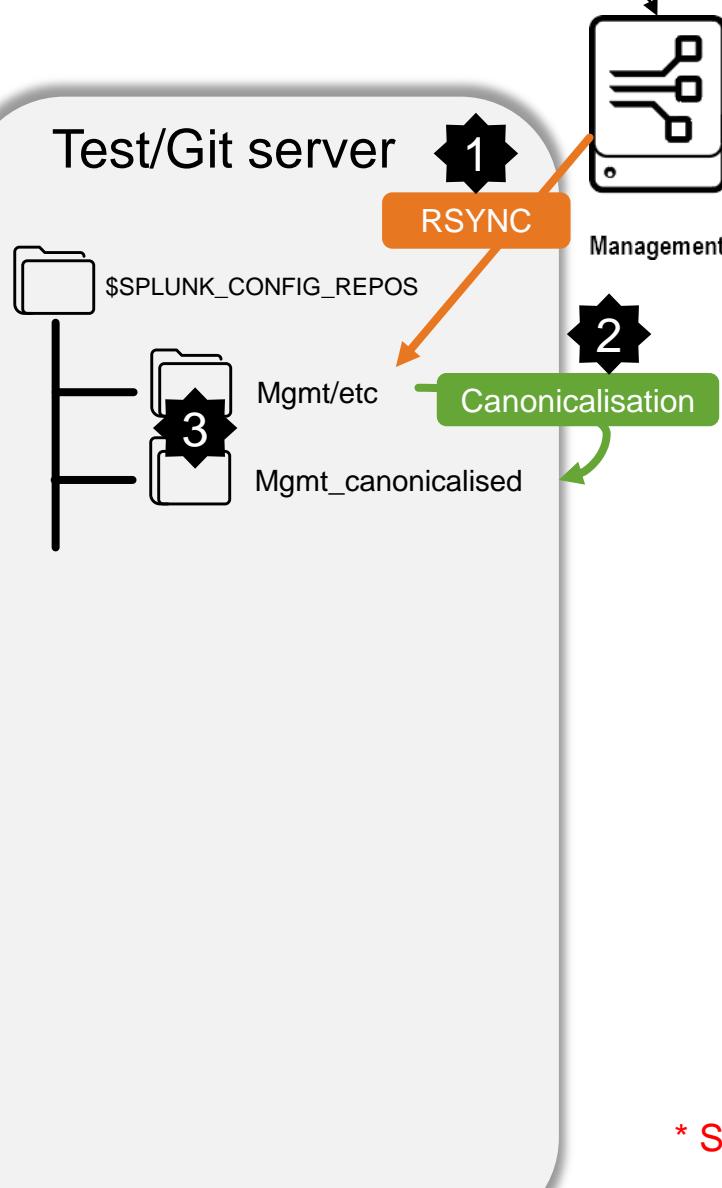
lookups/just_for_fun.csv	
1 - zzz,aaa	1 + aaa,zzz
2 - hello,bonjour	2 + bonjour,hello
3 - hi,au revoir	3 + "au revoir",goodbye
4 - hello world,bonjour tout le monde	4 + "bonjour tout le monde","hello world"
5 - hello world!,bonjour tout le monde!	5 + "bonjour tout le monde!","hello world!"

Change tracking

(not change control)



One example



Change tracking

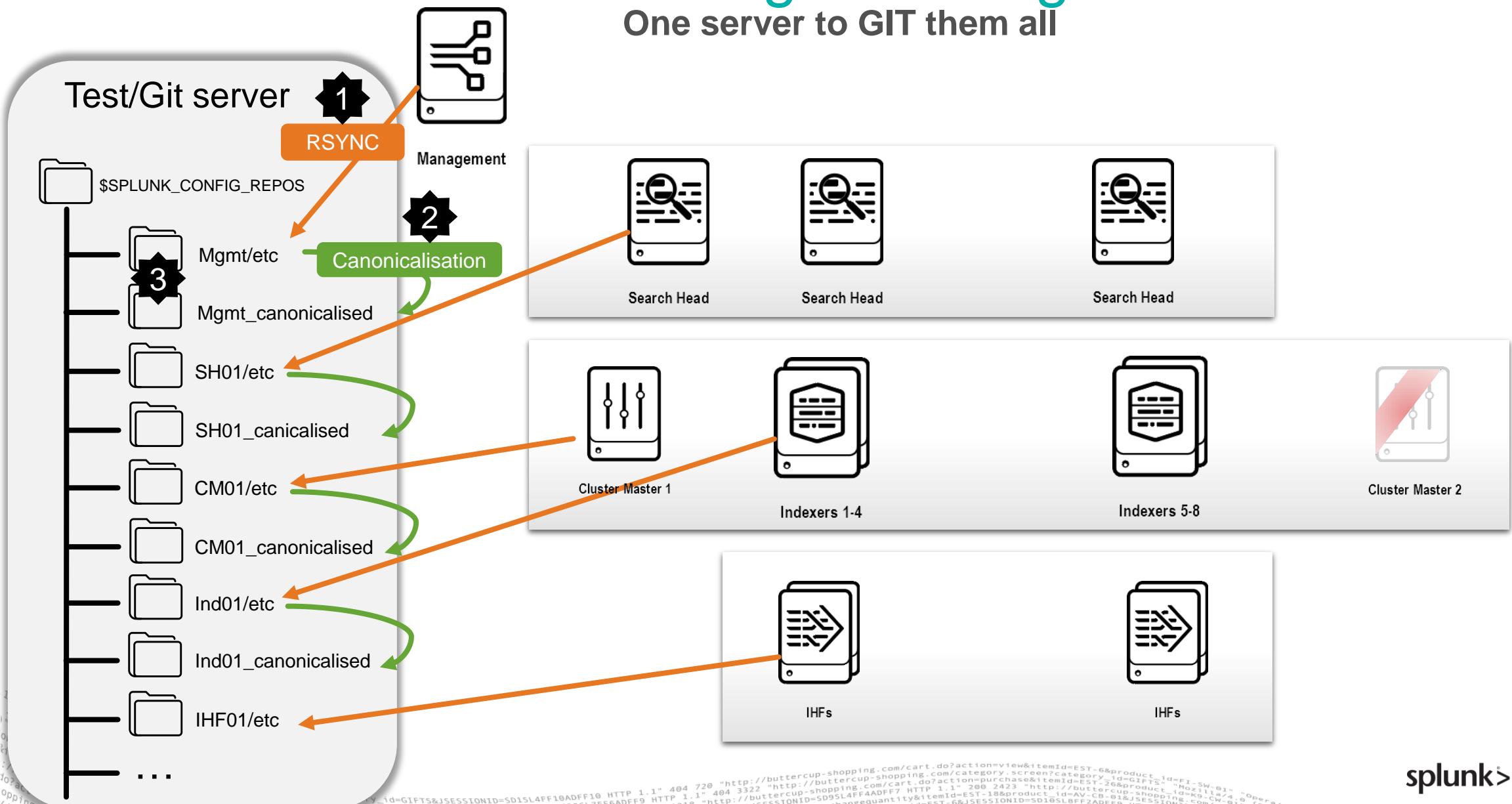
One server to GIT them all

- ▶ Rsync \$SPLUNK_HOME/etc
 - Exclude some files/folders* such as
 - Large csv files
 - Binaries or jars
 - Some folders: learned app or private object
- ▶ Canonicalise “Mgmt/etc” to “Mgmt_canonicalised”
- ▶ “Git” both folders
 - Beware of deleted files*

* See bonus slide

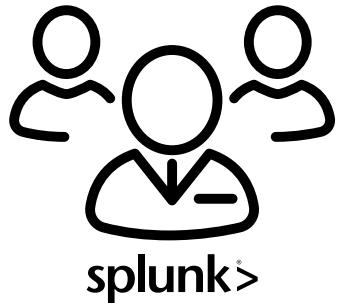
Change tracking

One server to GIT them all

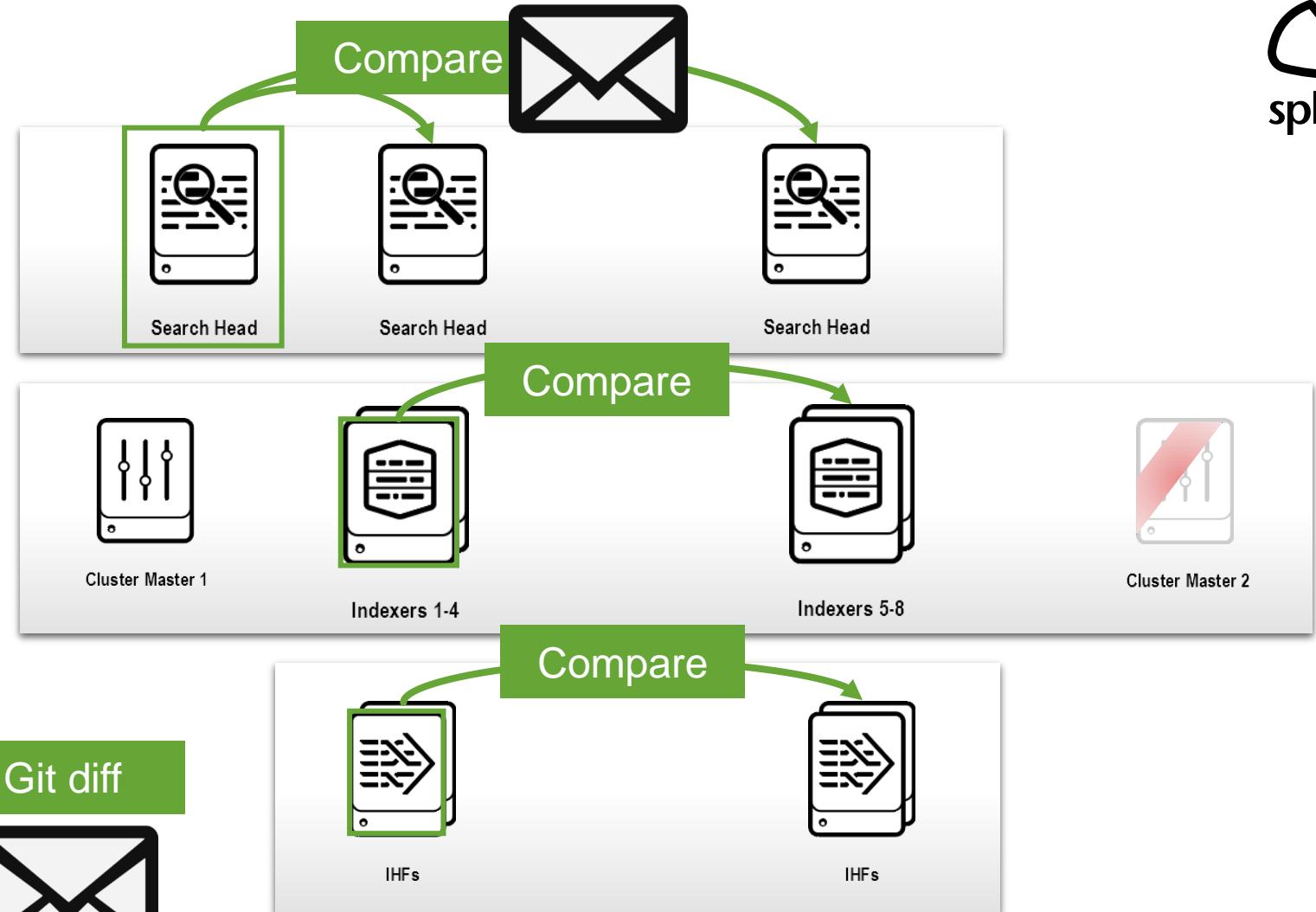
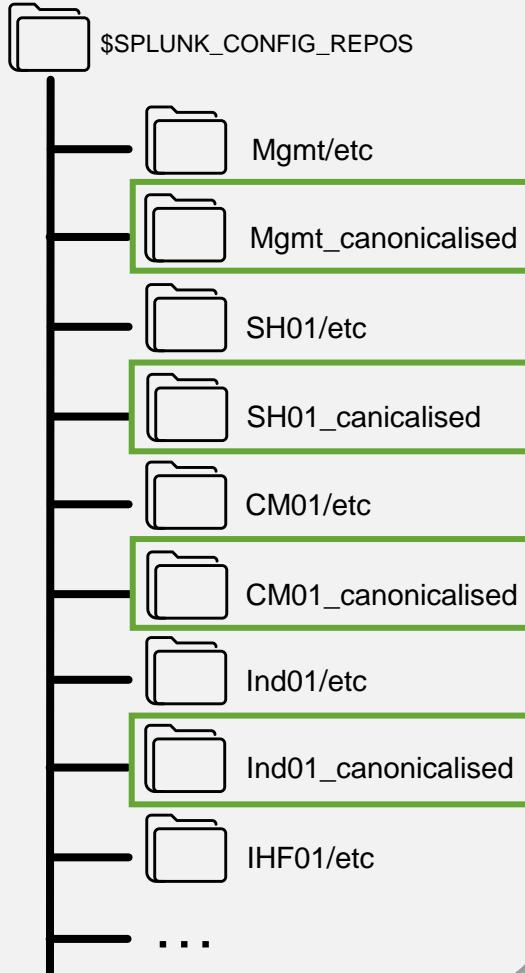


Change tracking

One server to GIT them all

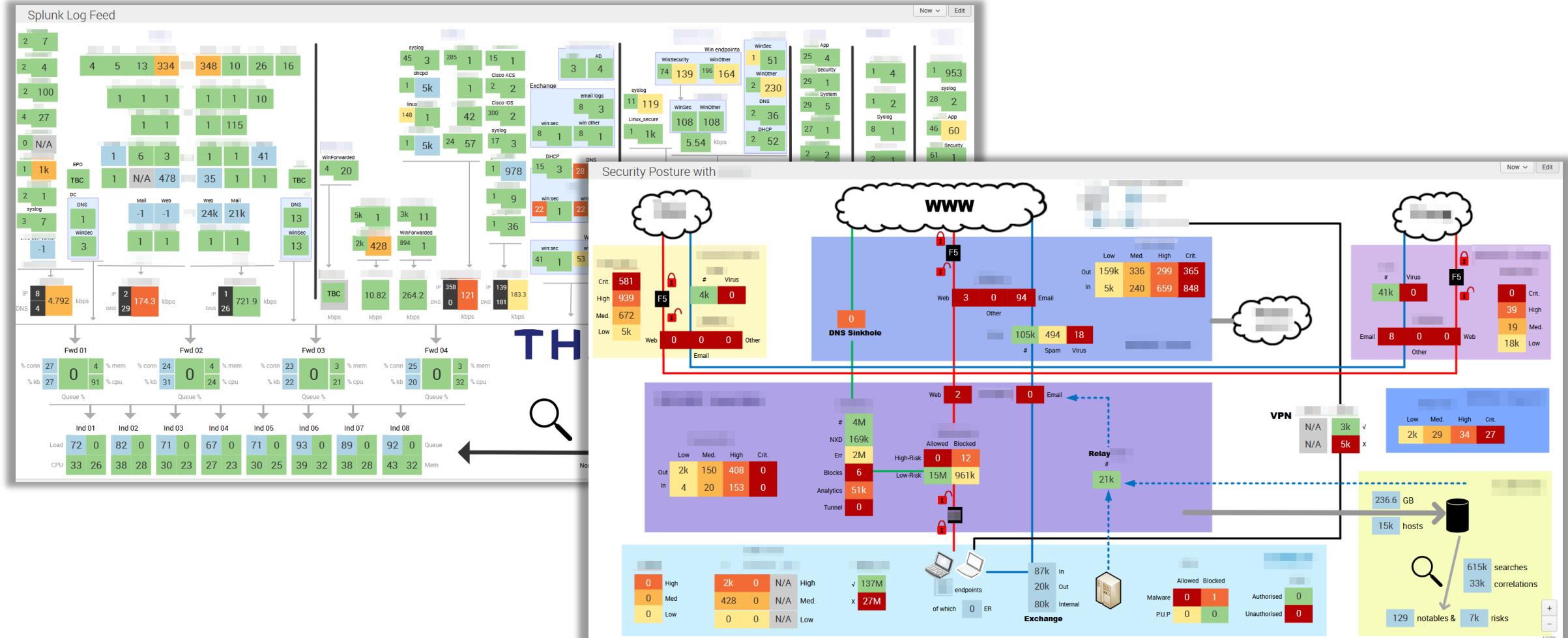


Test/Git server



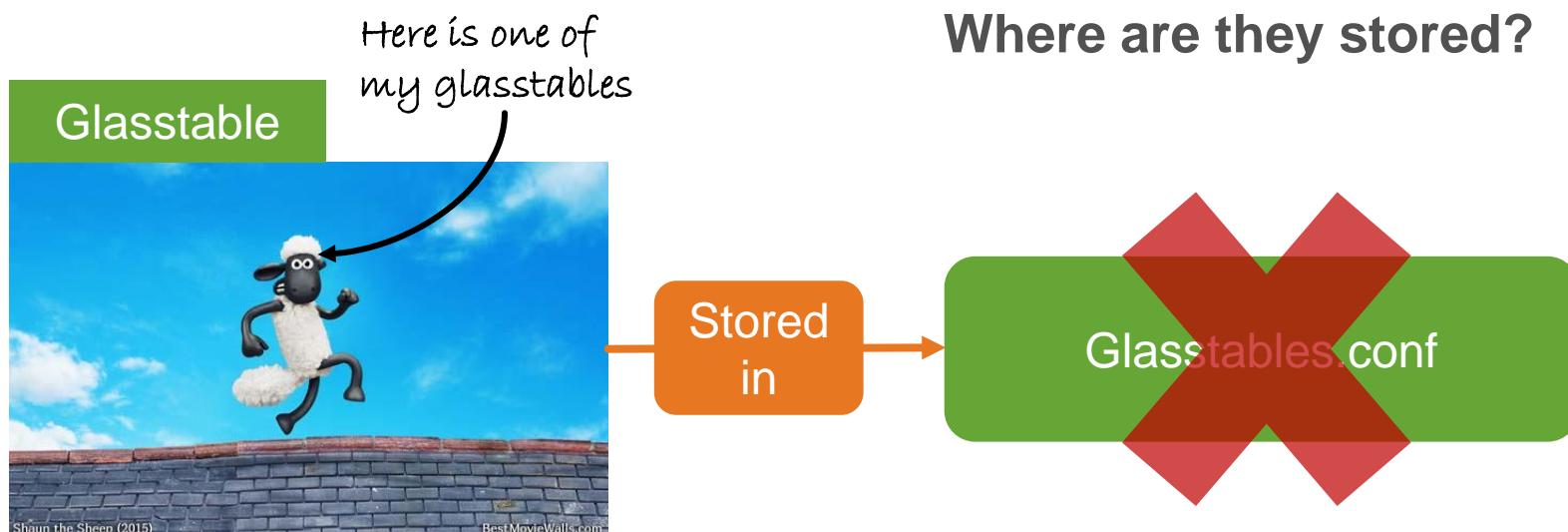
Glass tables

But have you forgotten your glasstables?



Glass tables

Where are they stored?



Glass tables



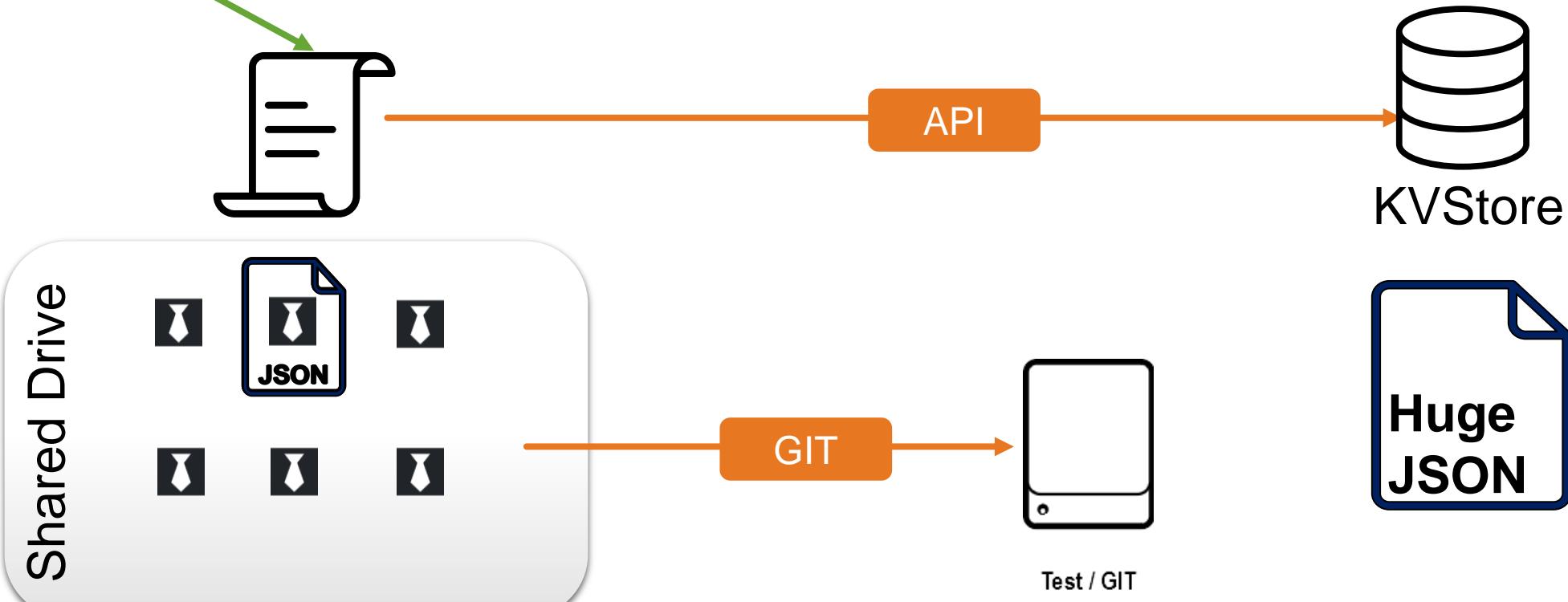
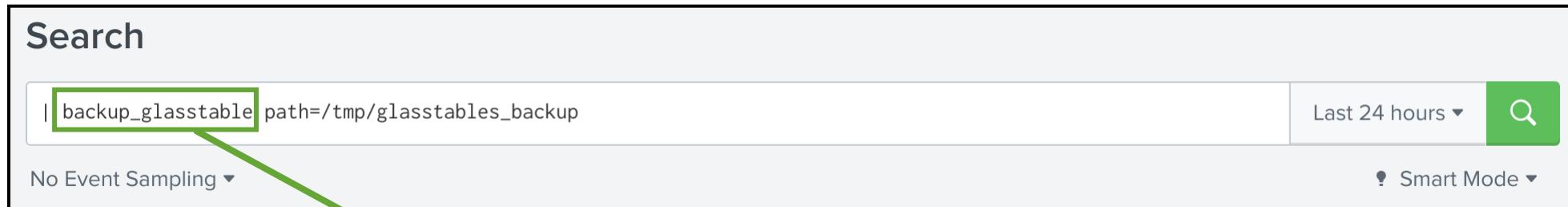
- ▶ Officially: You can **manually** export glasstables via the UI ... but it's manual!
- ▶ You can automate the backup of the **whole** KVStore. But:
 - Backup process is heavy (stop splunk, copy KVStore folder, start splunk)
 - Backup/Restore of KVStore is all or nothing (impact on Incident Review!)
- ▶ If you delete a glass table by mistake ... it is permanently deleted

```

138.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=update&productId=EST_26&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&product_id=AU-CUP-18&JSESSIONID=SD55L4FFAADDFF1 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_6&product_id=AU-CUP-18&JSESSIONID=SD55L8FF2ADFF1 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_19&product_id=AU-CUP-19&JSESSIONID=SD55L9FF3ADFF2 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_20&product_id=AU-CUP-20&JSESSIONID=SD55L9FF4ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_21&product_id=AU-CUP-21&JSESSIONID=SD55L9FF5ADFF5 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_22&product_id=AU-CUP-22&JSESSIONID=SD55L9FF6ADFF6 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_23&product_id=AU-CUP-23&JSESSIONID=SD55L9FF7ADFF7 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_24&product_id=AU-CUP-24&JSESSIONID=SD55L9FF8ADFF8 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_25&product_id=AU-CUP-25&JSESSIONID=SD55L9FF9ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_26&product_id=AU-CUP-26&JSESSIONID=SD55L9FF10ADFF10 HTTP 1.1" 200 3865
  
```

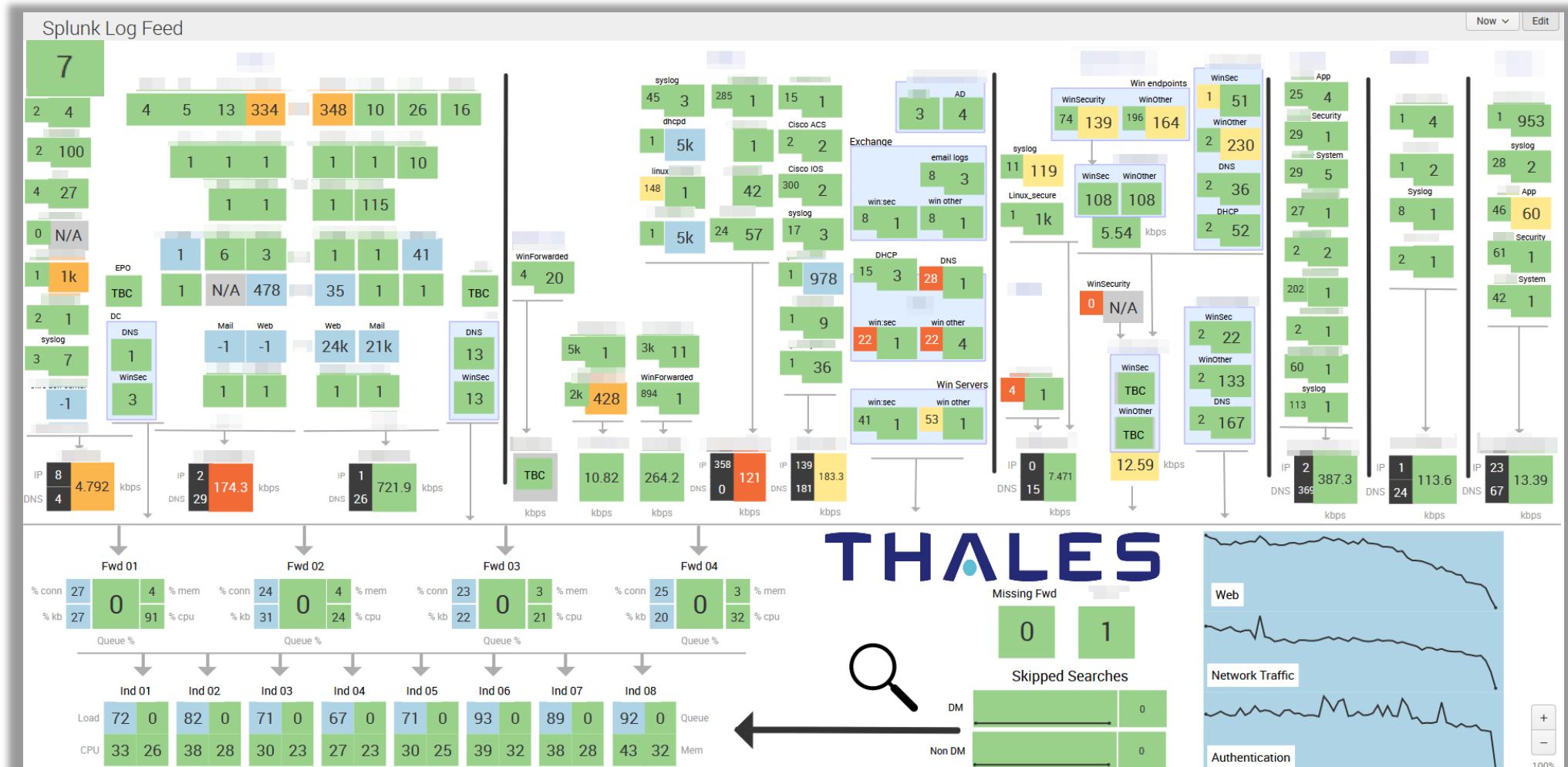
Glass tables

Our tracking/backup solution



Glass tables

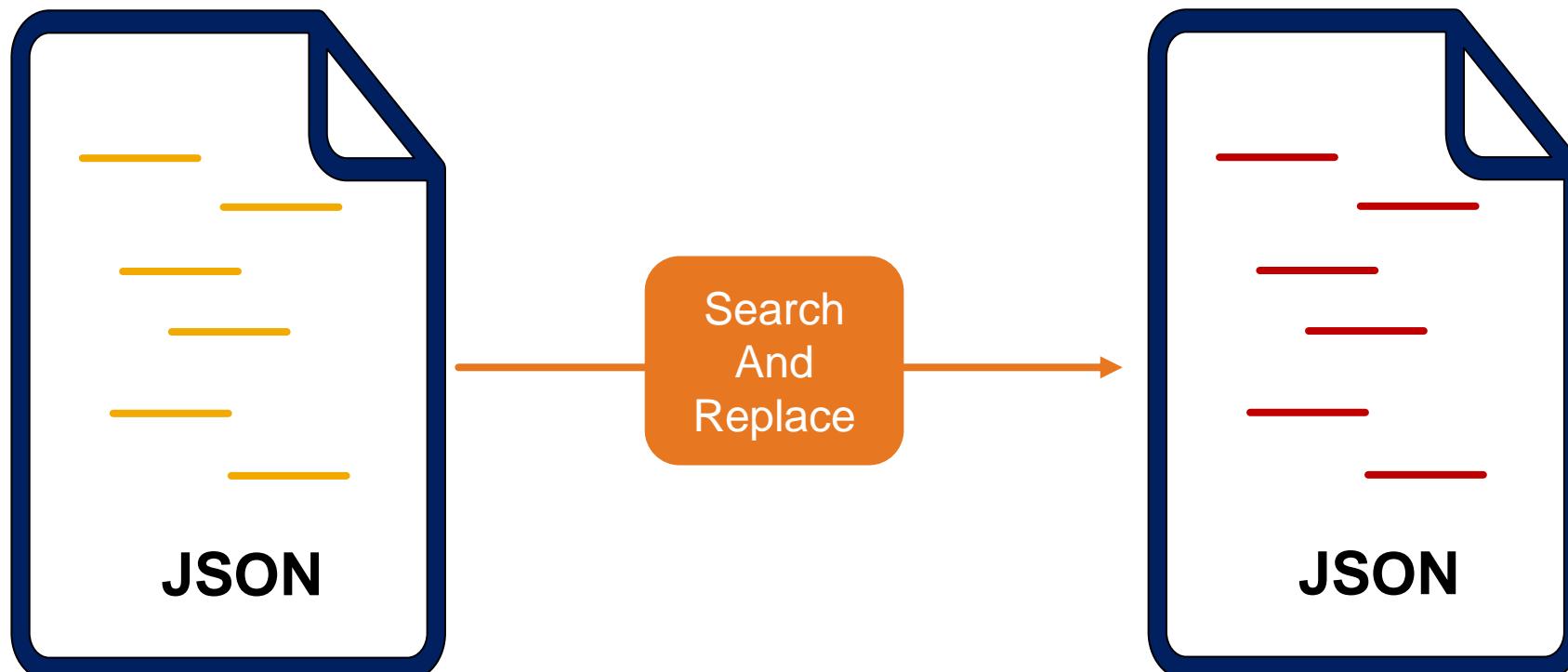
Tracking solution side effect



Glass tables

Tracking solution side effect

7 = | loadjob my_user:my_app:my_sched_search



Glass tables

Restore/deploy solution

SHC env



Single SH env



Just time for a quick recap

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ Tracking problem 1: precedence
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ **Track all changes (inc. glass tables)**
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades

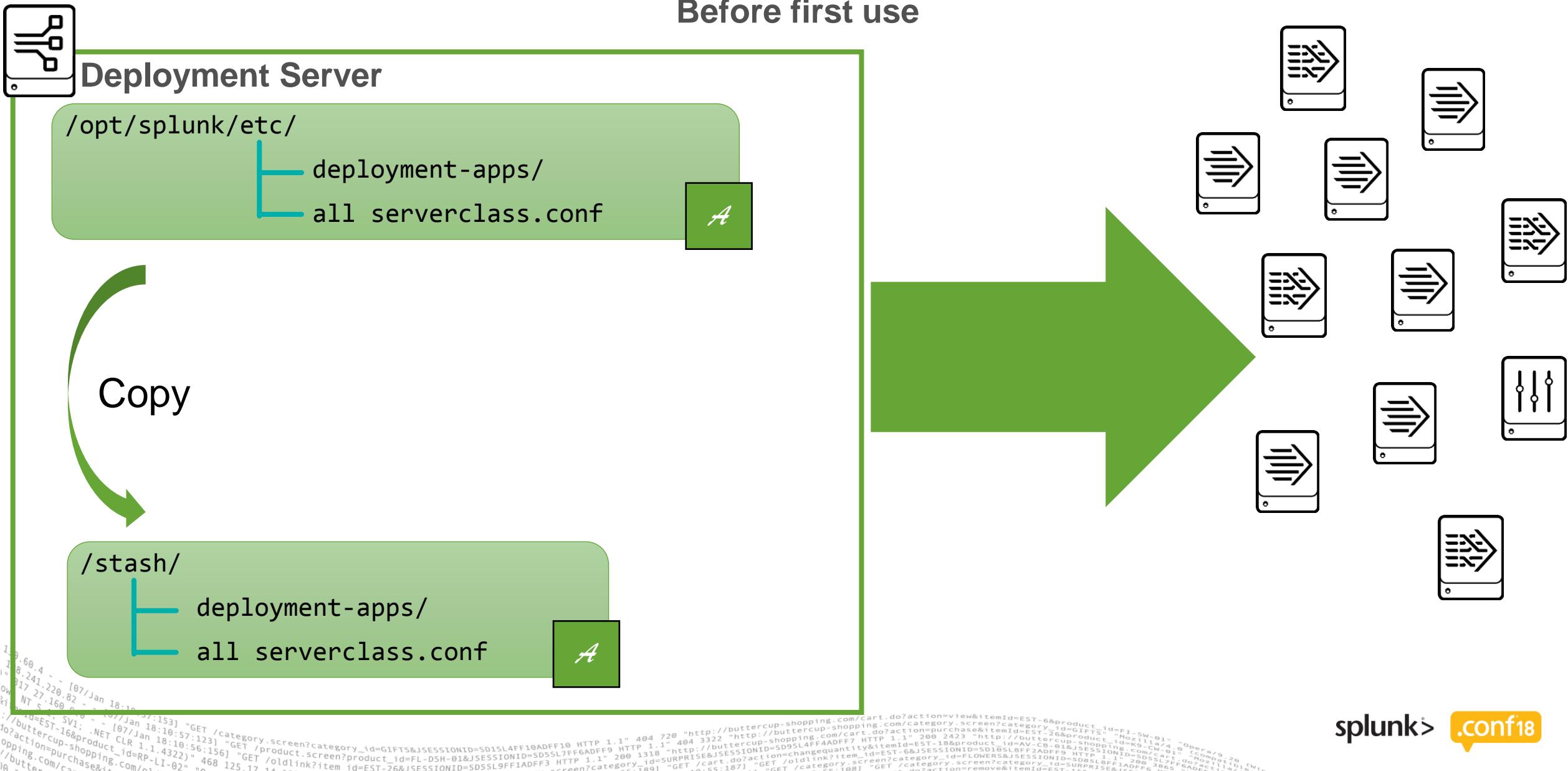


Deployment Server

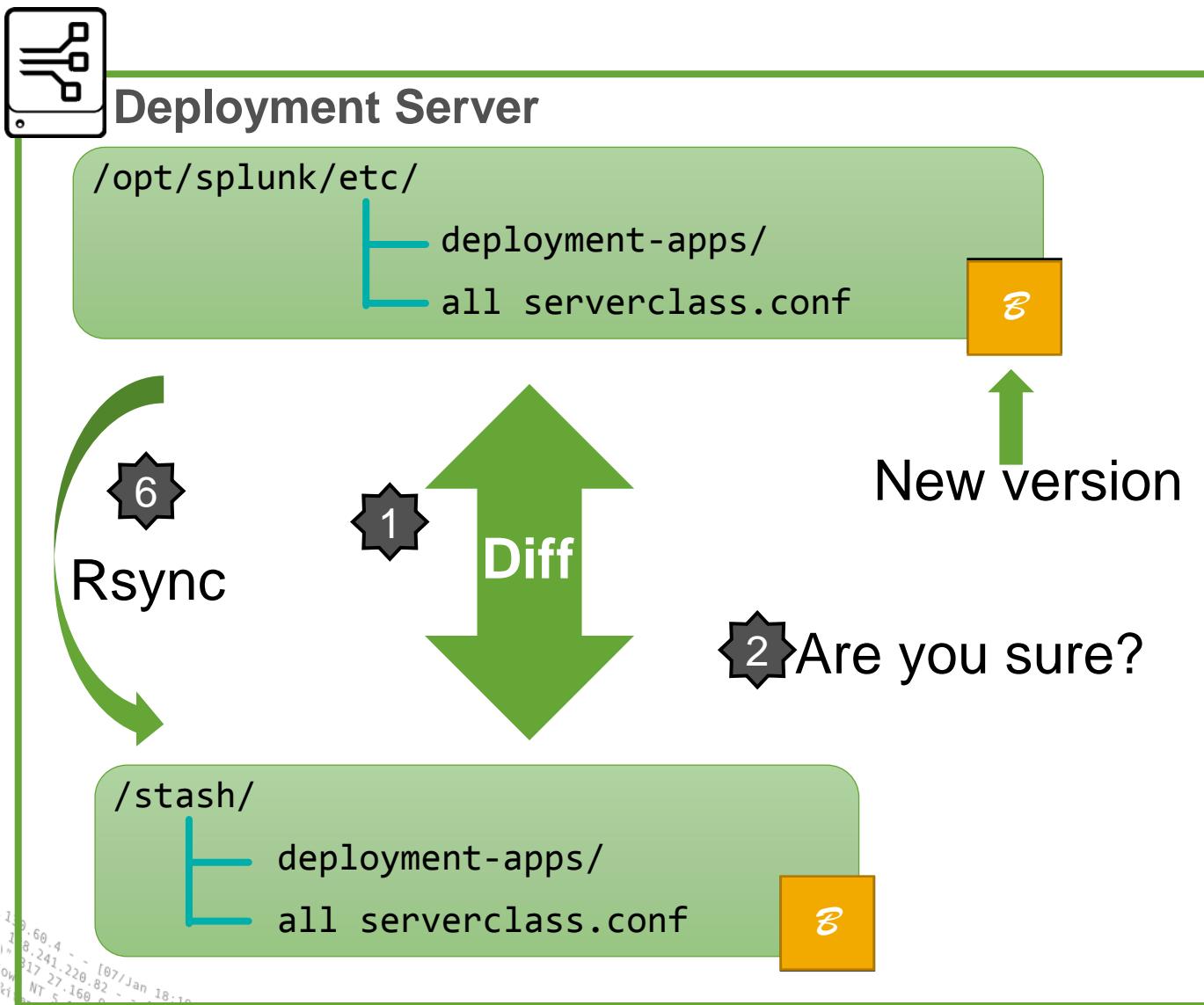


reload deploy-server wrapper v1

Before first use



reload deploy-server wrapper v1



⚠ Never deploy without the script!



④ Race condition / Friday check

③ Email diffs



reload deploy-server wrapper

Advantages

- ▶ Fairly easy to implement
- ▶ Avoid deploying other people's work-in-progress if they are not ready
- ▶ Can do peer review at the diff stage or after-the-fact with the email
- ▶ Good place to add more checks and balances

Disadvantages

- ▶ Requires discipline: never reload deploy-server directly
- ▶ Not ideal if you also use the Forwarder management Web UI to make changes
- ▶ May lie next time if the last step fails
- ▶ Doesn't actually know what's up with the deployment clients: trusts the stash is correct

reload deploy-server wrapper v2

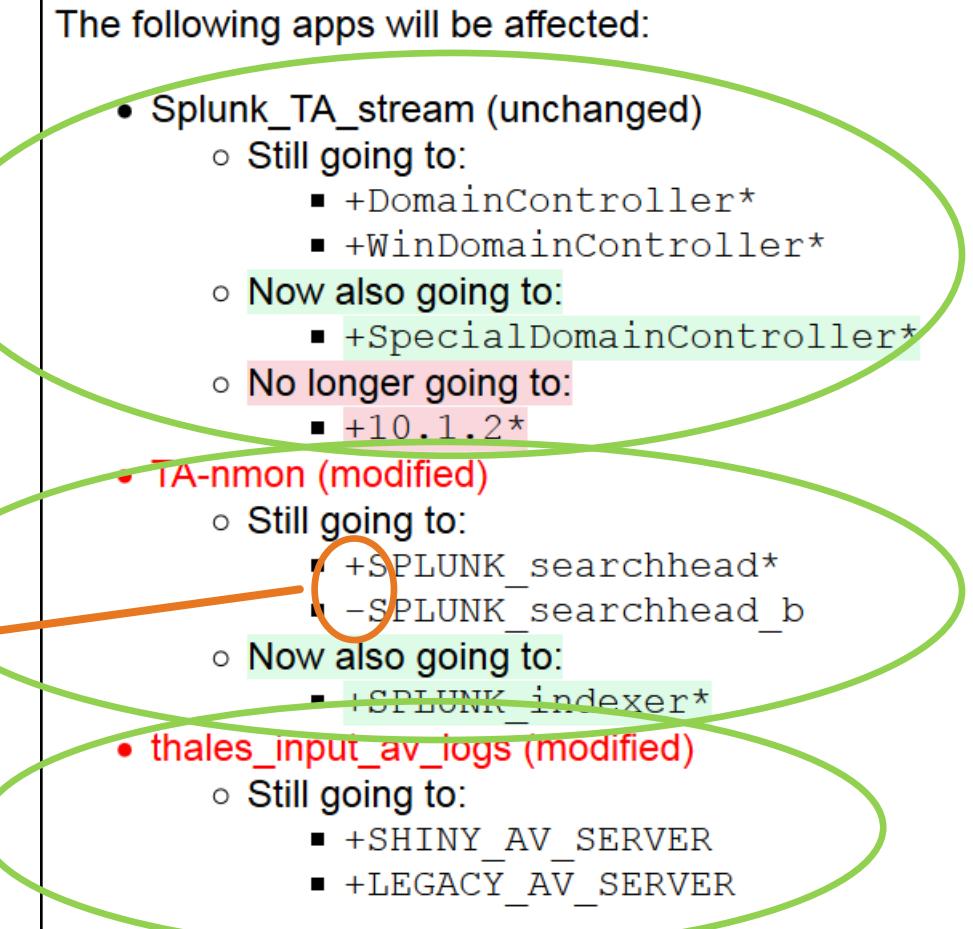
Summary = Most important improvement!

- ▶ parse before and after server classes
- ▶ compute which server classes are affected
- ▶ deduce which apps are affected
- ▶ parse deployment-apps diff: compute which apps are changed
- ▶ put this together and compute summary

Serverclass.conf example:

```
[serverClass:Monitored_Splunk]
whitelist.0=SPLUNK_searchhead*
blacklist.0=SPLUNK_searchhead_b
whitelist.1=SPLUNK_indexer*
```

[serverClass:Monitored_Splunk:app:TA-nmon]



reload deploy-server wrapper v3

Make it fancy

- ▶ inputs.conf catch-all review and suggestions

The Critical Syslog Tricks That No One Seems to Know About

Wednesday, September 27, 2017 | 4:35 PM-5:20 PM ADVANCED

George Barrett, Splunk Consultant, Rational Cyber

Jonathan Margulies, Splunker. Co-author of textbook "Security in Computing",
Department of Justice

- ▶ Naming convention check/enforcement for new apps

- ▶ ...

apply cluster-bundle script

- ▶ You can do the same on your Cluster Master for your indexer cluster.
- ▶ Even simpler since no serverclass complexity.
- ▶ Just stash /opt/splunk/etc/master-apps/

Just time for a quick recap

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ Tracking problem 1: precedence
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ Track all changes (inc. glass tables)
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades

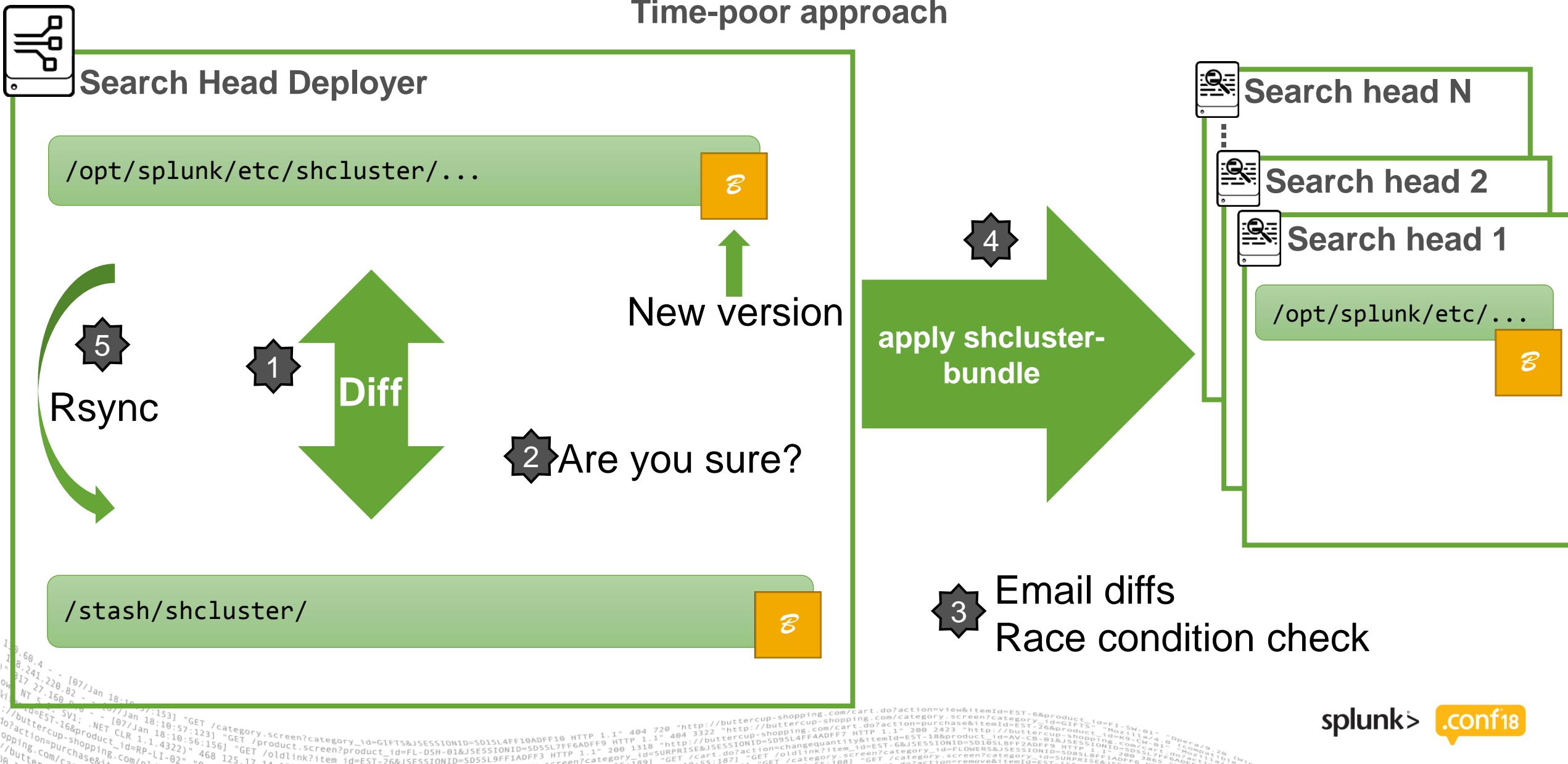


Search Head Deployer



apply shcluster-bundle wrapper v1

Time-poor approach



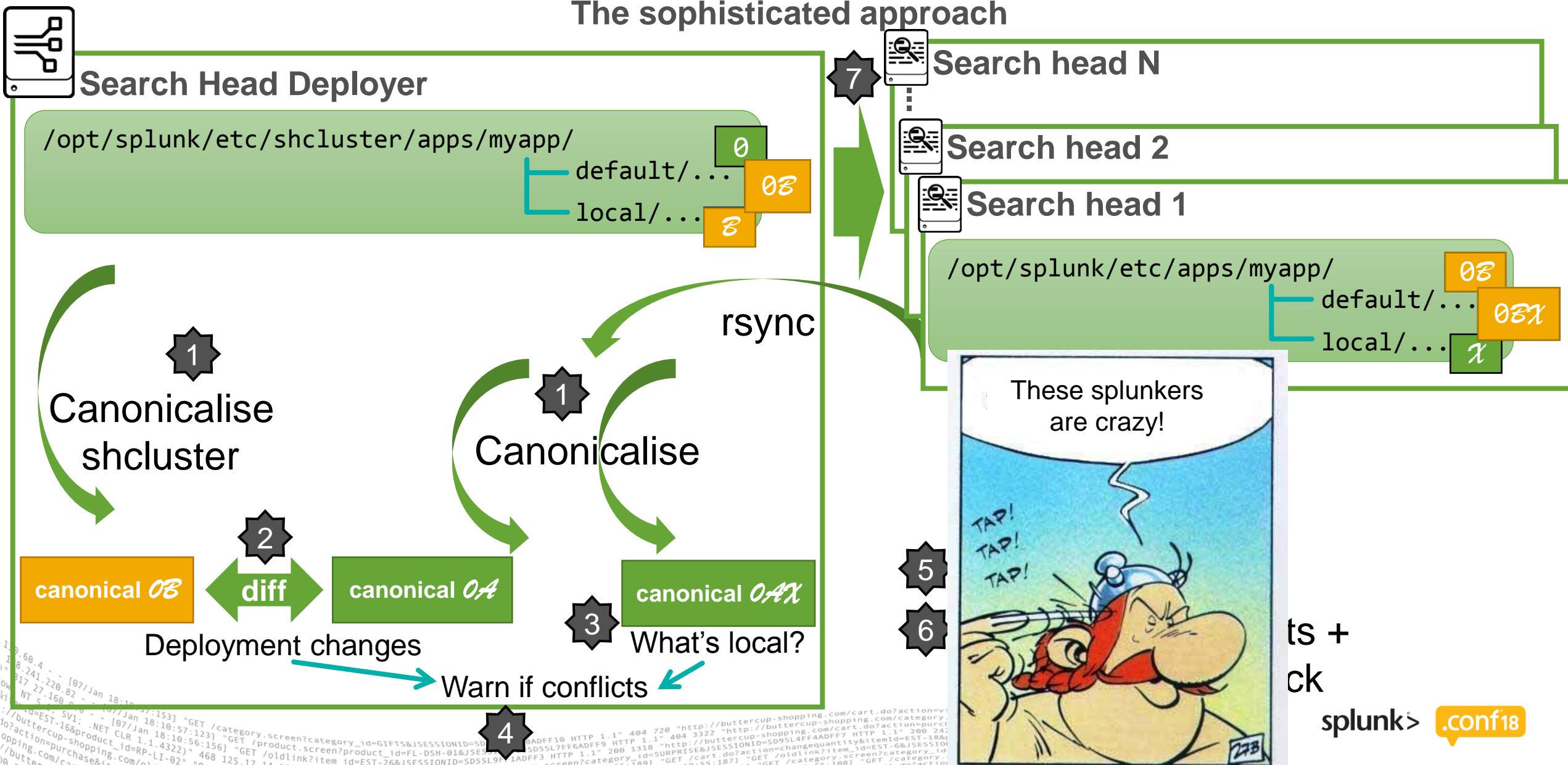
apply shcluster-bundle wrapper v1

Advantages

Disadvantages

- ▶ Easy
 - ▶ Doesn't know what's up with the search heads

apply shcluster-bundle wrapper v2



apply shcluster-bundle wrapper v2

Advantages

- ▶ Accurately predict actual effective change!
 - ▶ Accurate even if other changes have happened (e.g. direct apply shcluster-bundle)
 - ▶ Warm fuzzy feeling for control freaks

Disadvantages

- ▶ Slow (rsync + canonical = 1 minute)
 - ▶ Fair amount of work to implement

Just time for a quick recap

- ▶ Intro - Us and our environment
 - ▶ Full change control is heavy: just track
 - ▶ Tracking problem 1: precedence
 - ▶ Canonical configuration
 - ▶ Tracking problem 2: diff explosions
 - ▶ Track all changes (inc. glass tables)
 - ▶ Control deployment server deployments
 - ▶ **Control search head deployments**
 - ▶ Control upgrades



Control upgrades



Precedence + upgrades = recipe for disaster

- Later we upgrade Splunk_SA_CIM from version A to version B:

Search Head

```
/opt/splunk/etc/apps/Splunk_SA_CIM/
```

```
    └── default/data/models/Malware.json
```

constraint: tag=malware tag=attack
fields: ...
....

A

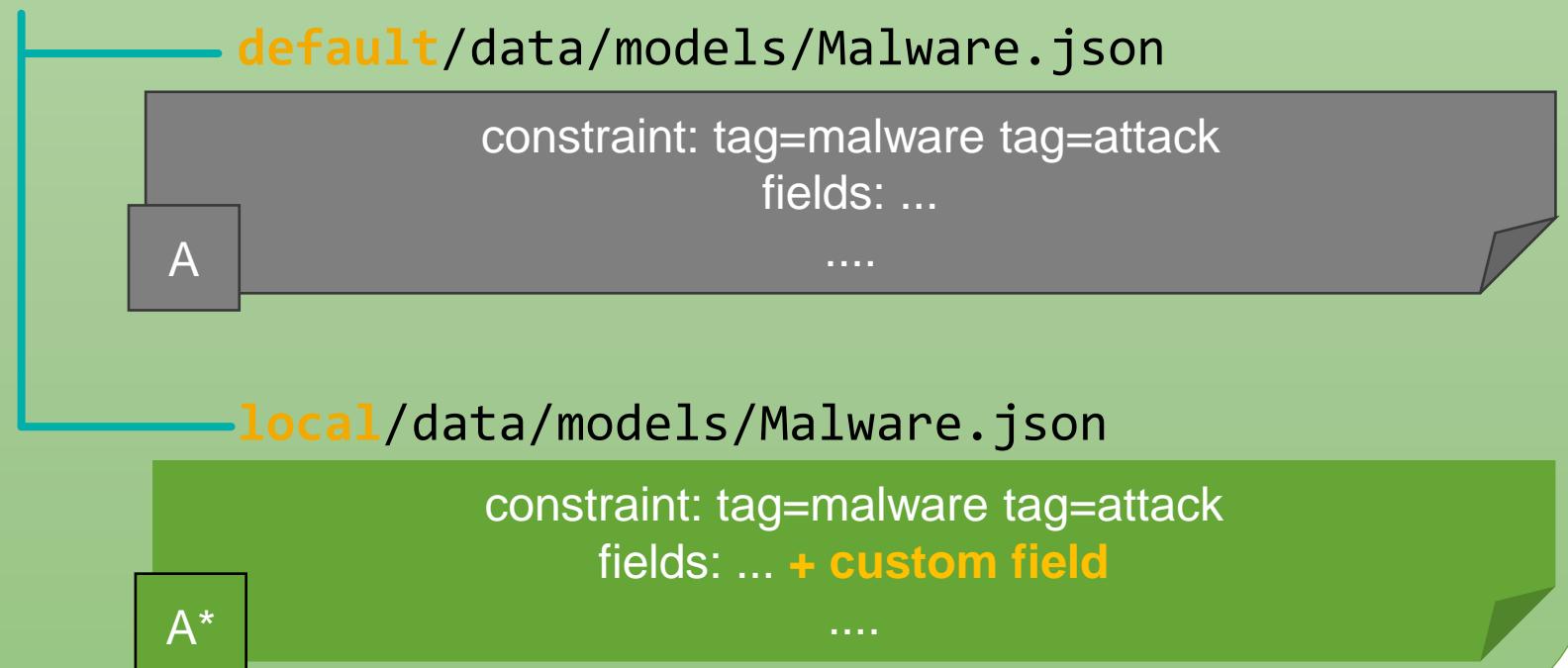
```
138 60.4 ~ [07/Jan/18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.19 ://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-16&product_id=RP-LI-02 "o~ [07/Jan/18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 131@ "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST-18&product_id=AU-CCE-18&JSESSIONID=SD08SLBFF2ADFF4 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity?itemId=EST_6&SESSIONID=SD10SLBFF2ADFF4 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove?itemId=EST_10&SESSIONID=SD08SLBFF2ADFF4 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST_10&SESSIONID=SD08SLBFF2ADFF4 HTTP 1.1" 200 3865
```

Precedence + upgrades = recipe for disaster

- Later we upgrade Splunk_SA_CIM from version A to version B:

Search Head

/opt/splunk/etc/apps/Splunk_SA_CIM/

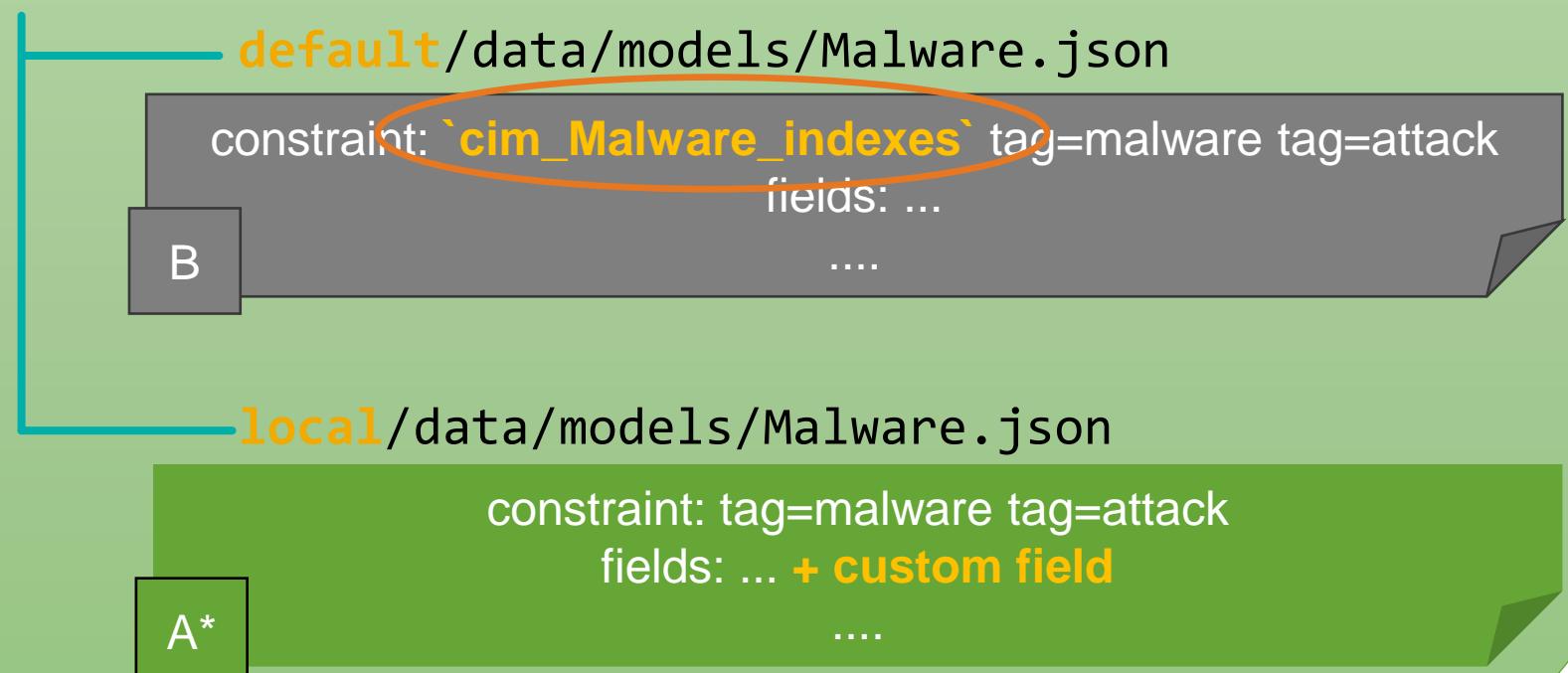


Precedence + upgrades = recipe for disaster

- Later we upgrade Splunk_SA_CIM from version A to version B:

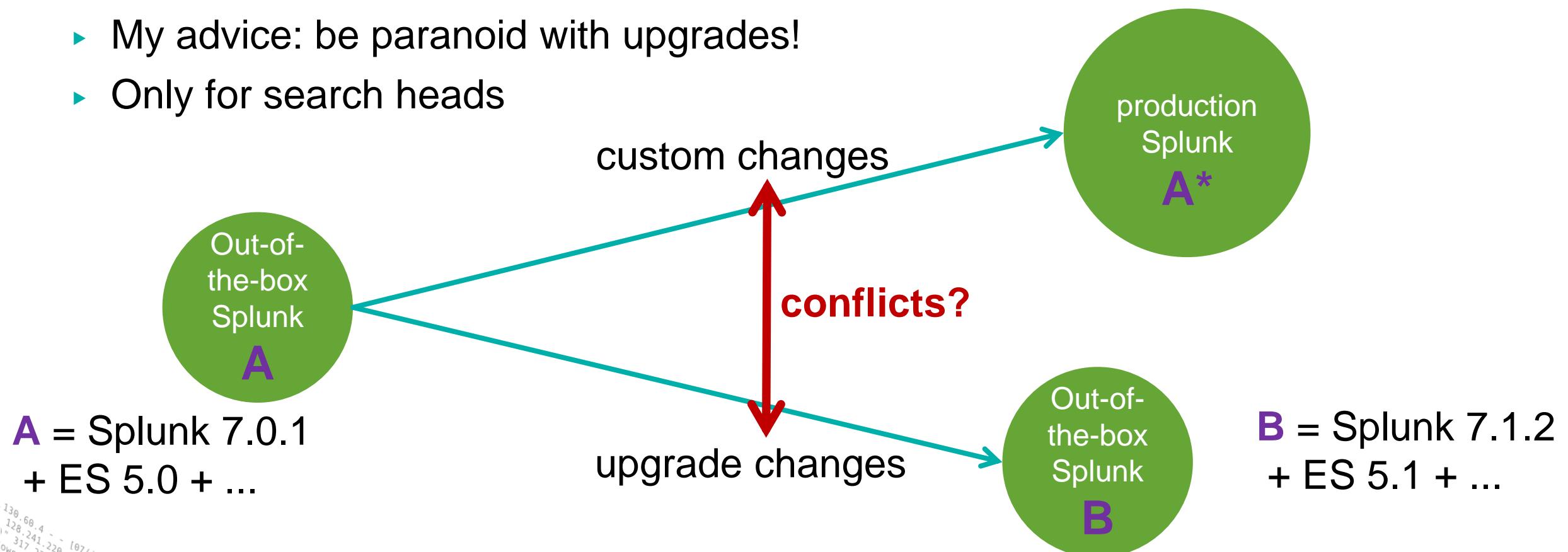
Search Head

/opt/splunk/etc/apps/Splunk_SA_CIM/

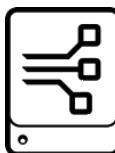


Upgrade strategy

- ▶ The advice you hear: "clone before you modify"
 - I don't see the point as it doesn't solve the problem
- ▶ My advice: be paranoid with upgrades!
- ▶ Only for search heads

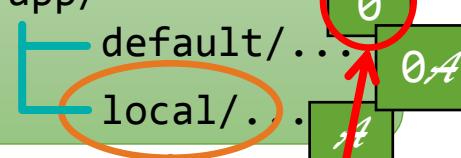


Pre-upgrade report script



Search Head Deployer

/opt/splunk/etc/shcluster/apps/myapp/

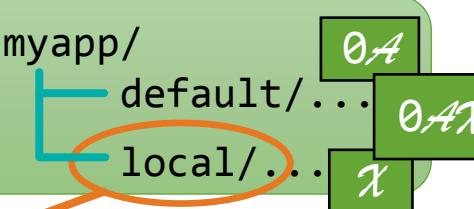


Search head N

Search head 2

Search head 1

/opt/splunk/etc/apps/myapp/



conflicts?

upgrade
changes

diff

1 VS χ
conflicts!

Out-of-the-box* current

/opt/splunk/etc/apps/myapp/default/...



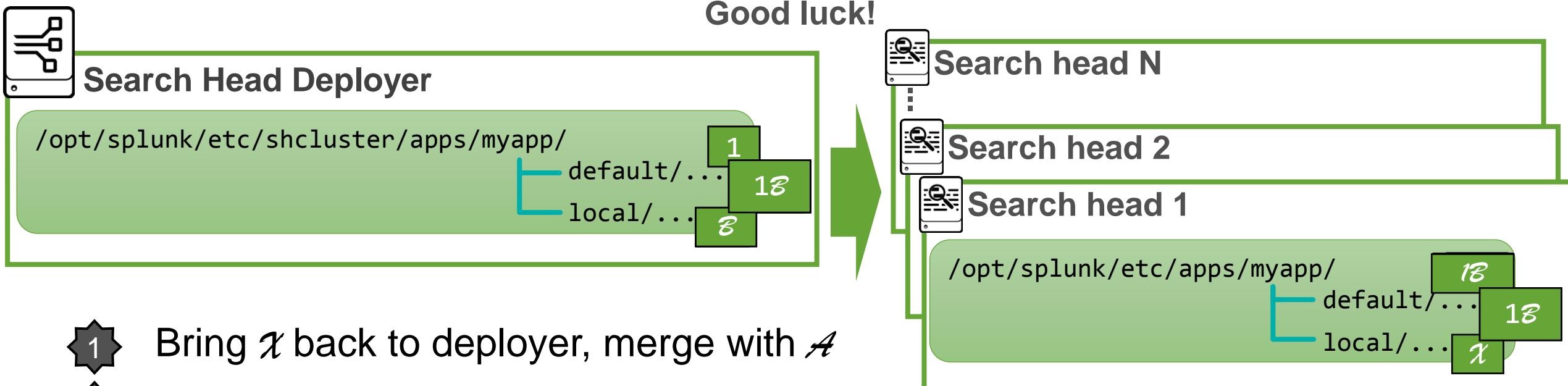
Out-of-the-box* future

/opt/splunk/etc/apps/myapp/default/...

1

* See bonus slide

Fixing upgrade conflict on a search head cluster



- 1 Bring χ back to deployer, merge with \mathcal{A}
- 2 Deploy $0\mathcal{A}\chi$
- 3 Remove local χ on search heads
- 4 Upgrade on deployer
- 5 Fix any conflicts between $0\mathcal{A}\chi$ and 1 with $1\mathcal{B}$
- 6 Deploy $1\mathcal{B}$

Just time for a quick recap

- ▶ Intro - Us and our environment
- ▶ Full change control is heavy: just track
- ▶ Tracking problem 1: precedence
- ▶ Canonical configuration
- ▶ Tracking problem 2: diff explosions
- ▶ Track all changes (inc. glass tables)
- ▶ Control deployment server deployments
- ▶ Control search head deployments
- ▶ Control upgrades



WE FEAR CHANGE

Conclusions

"It's a dangerous business, Frodo, going out your door. You step onto the road, and if you don't keep your feet, there's no knowing where you might be swept off to."



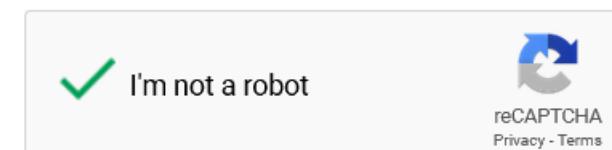
Last words

Take out

- ▶ Some things are easy to do and bring a lot of value
- ▶ With some significant coding you can enrich things further a long way

Words of caution

- ▶ Splunk is complicated: taking everything into account is difficult
- ▶ Splunk can change: future versions might be completely different
- ▶ Splunk is many: know the particularities of your setup
- ▶ Don't trust the robots: scripts can save your bacon but don't blindly trust them



Q & A

Thank you!

1. Slides and recording available on <http://conf.splunk.com/sessions/2018-sessions.html> in a few days/weeks
2. Slides and material available now at <https://bit.ly/TrackSplunk>
3. Rate this session in the app :-)
4. Poke us if you see us in the airport!
Gabriel Vasseur & Olivier Lauret

Bonus slides



rsync include pattern

```
rsync -avz myserver:/opt/splunk/etc/ /var/tmp/myserver/  
--prune-empty-dirs --exclude-from=<PATTERN_FILE>
```

```
- *.index
- README
- samples
- *.tmp
- *
- *.old
- *.context.csv
- *.context.csv.default
- *_tracker.csv
- *_tracker2.csv
- *_tracker.csv.default
- *_tracker2.csv.default
- *.pyc
- *.pyo
- *.spl
- *.tgz
- *.tar.gz
- apps/*/default.old*
- jars
- *_x86_*
- app_common
- *_app_common
- install
- /etc/users/**
- /etc/apps/learned/**
+ *.conf
+ *.meta
+ /etc/*
+ /etc/system/bin/*
+ /etc/system/lookups/*
+ /etc/system/local/**
+ /etc/system/default/data/**
+ /etc/apps/*/*bin/*
+ /etc/apps/*/*lookups/*
+ /etc/apps/*/*local/**
+ /etc/apps/*/*default/data/**
+ /shcluster/apps/*/*bin/*
+ /shcluster/apps/*/*lookups/*
+ /shcluster/apps/*/*local/**
+ /shcluster/apps/*/*default/data/**
+ /etc/auth/**
+ /etc/licenses/**
+ /etc/modules/**
+ /etc/slave-apps/**
+ /etc/master-apps/**
+ /etc/deployment-apps/**
+ /etc/shcluster/***
***
```

Change tracking: putting in git

- ▶ “rsync --delete” to Mgmt/etc
- ▶ Delete all files in the Mgmt/etc_canonicalised folder (except the .git folder)
- ▶ Use canonicalise script to create Mgmt/etc_canonicalised from Mgmt/etc
- ▶ Then git both folders but don't forget deleted files:

```

cd $SPLUNK_CONFIG_REPOS
# Run through all repos
for REPO in `./bin/ls $SPLUNK_CONFIG_REPOS` ; do
    cd $SPLUNK_CONFIG_REPOS/$REPO ;
    for DELETED_FILE in `git status --porcelain | egrep "^\ D " | sed "s/ \ D //"` ; do
        git rm $DELETED_FILE;
    done
    git add *
    git commit -m "Automated commit on `date +\"%Y-%m-%dT%T\"`"
    git push origin HEAD
    cd $SPLUNK_CONFIG_REPOS
done

```

Glass tables

Our tracking/backup solution

- ▶ The backup is orchestrated by a **custom search command** scheduled daily
- ▶ The script behind gets the glasstables definition via the Splunk API
 - 2 collectors in the KVStore to retrieve as 2 big json files:
 - `SplunkEnterpriseSecuritySuite_glasstables`
 - `/servicesNS/nobody/SplunkEnterpriseSecuritySuite/storage/collections/data/SplunkEnterpriseSecuritySuite_glasstables?limit=0&count=0&output_mode=json`
 - `SplunkEnterpriseSecuritySuite_files` (include images)
 - `/servicesNS/nobody/SplunkEnterpriseSecuritySuite/storage/collections/data/SplunkEnterpriseSecuritySuite_files?limit=0&count=0&output_mode=json`
 - ▶ Each big json file is split, prettified and saved into discrete json files corresponding to individual glass tables or their dependencies.
 - ▶ Each discrete json file is saved on a shared location available to the GIT server

We then GIT the shared location and pushed into Gitlab

Out-of-the-box splunk + ES

Faking it: no need to run anything, just unpack

- ▶ Unpack splunk core tgz /var/tmp/
- ▶ Unpack enterprise security tgz in /var/tmp/splunk/etc/apps/
- ▶ Unpack *.tgz and *.spl from /var/tmp/splunk/etc/apps/SplunkEnterpriseSecuritySuite/install/ in /var/tmp/splunk/etc/apps/
- ▶ Remove *.tgz and *.spl from /var/tmp/splunk/etc/apps/SplunkEnterpriseSecuritySuite/install/
- ▶ Unpack any other TA or app spl in /var/tmp/splunk/etc/apps/
- ▶ Rename any .csv.default to .csv
- ▶ Make /var/tmp/splunk/etc/system/default/authentication.conf readable
- ▶ Remove any bundled TA that you don't have in production
- ▶ Check that you have the same apps and versions as production