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

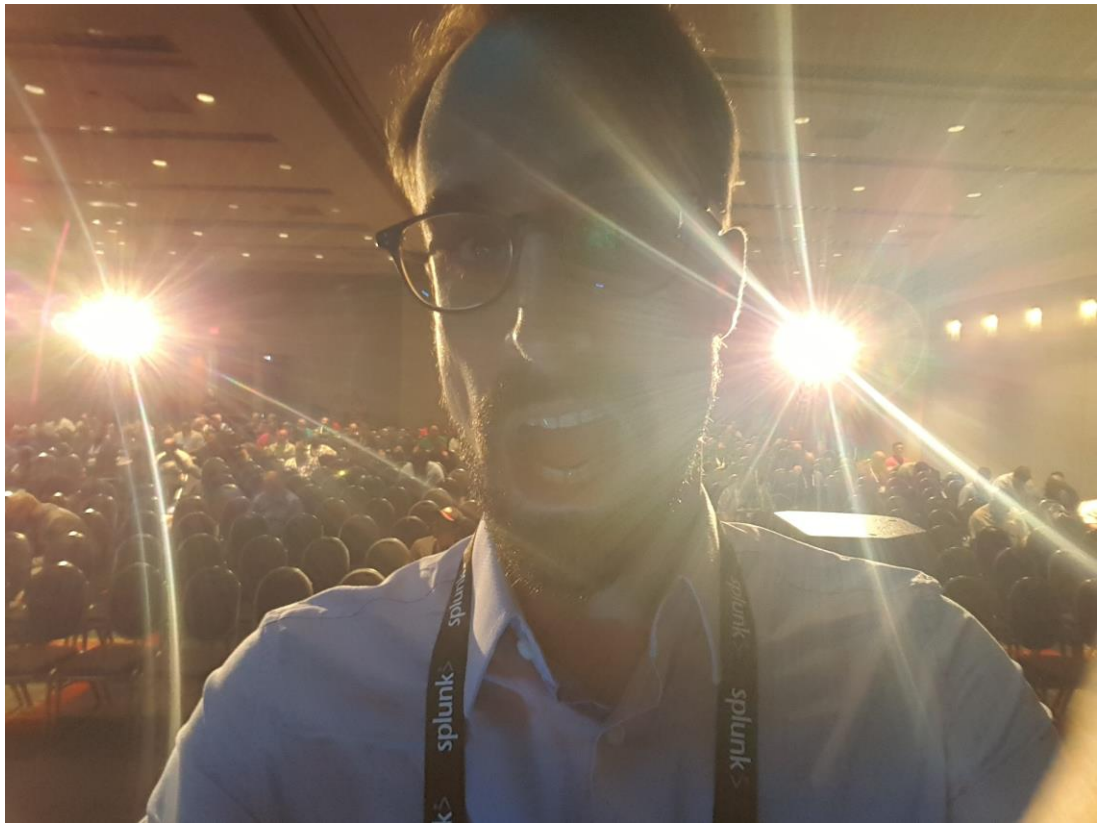
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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> .conf18

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!

splunk> .conf18

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)

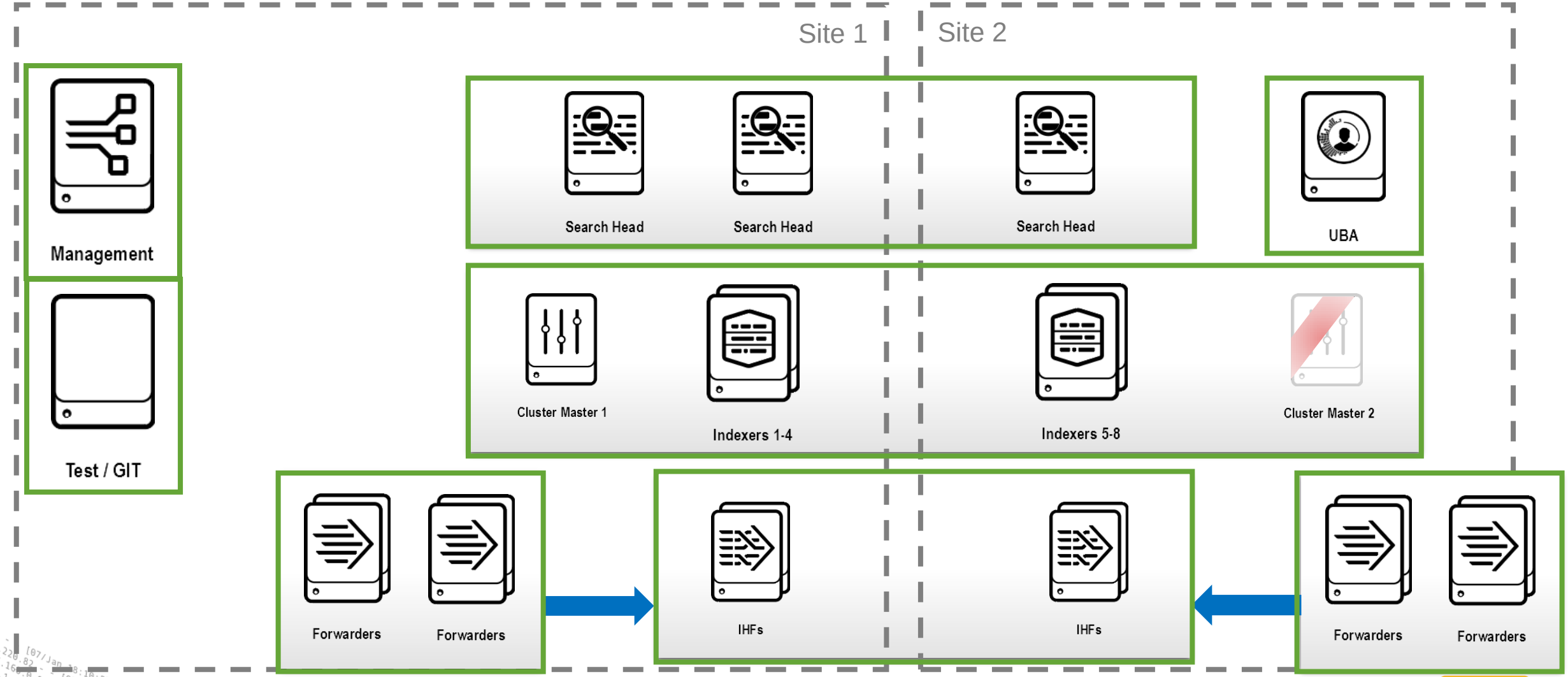
  Best company in the world (no doubt!)

  - 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

splunk> .conf18

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

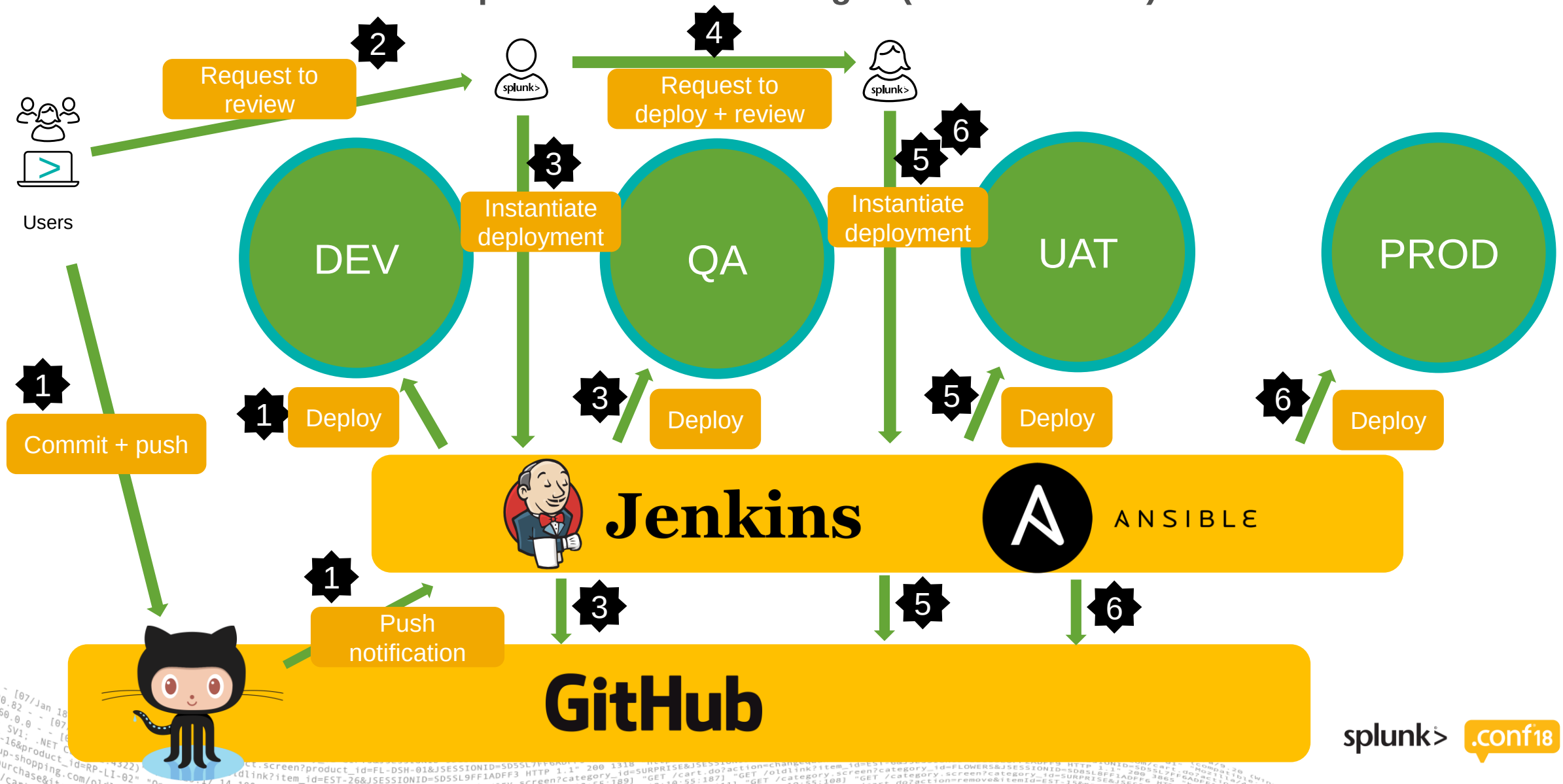
- Intro - Us and our environment
- Full change control is heavy: just track
- Tracking problem 1: precedence
- Canonical configuration
- Tracking problem 2: diff explosions
- Track all changes (inc. glass tables)
- Control deployment server deployments
- Control search head deployments
- Control upgrades

Proper Change Control is heavy

splunk> .conf18

The heavy solution

Complete control on changes (NOT at Thales)

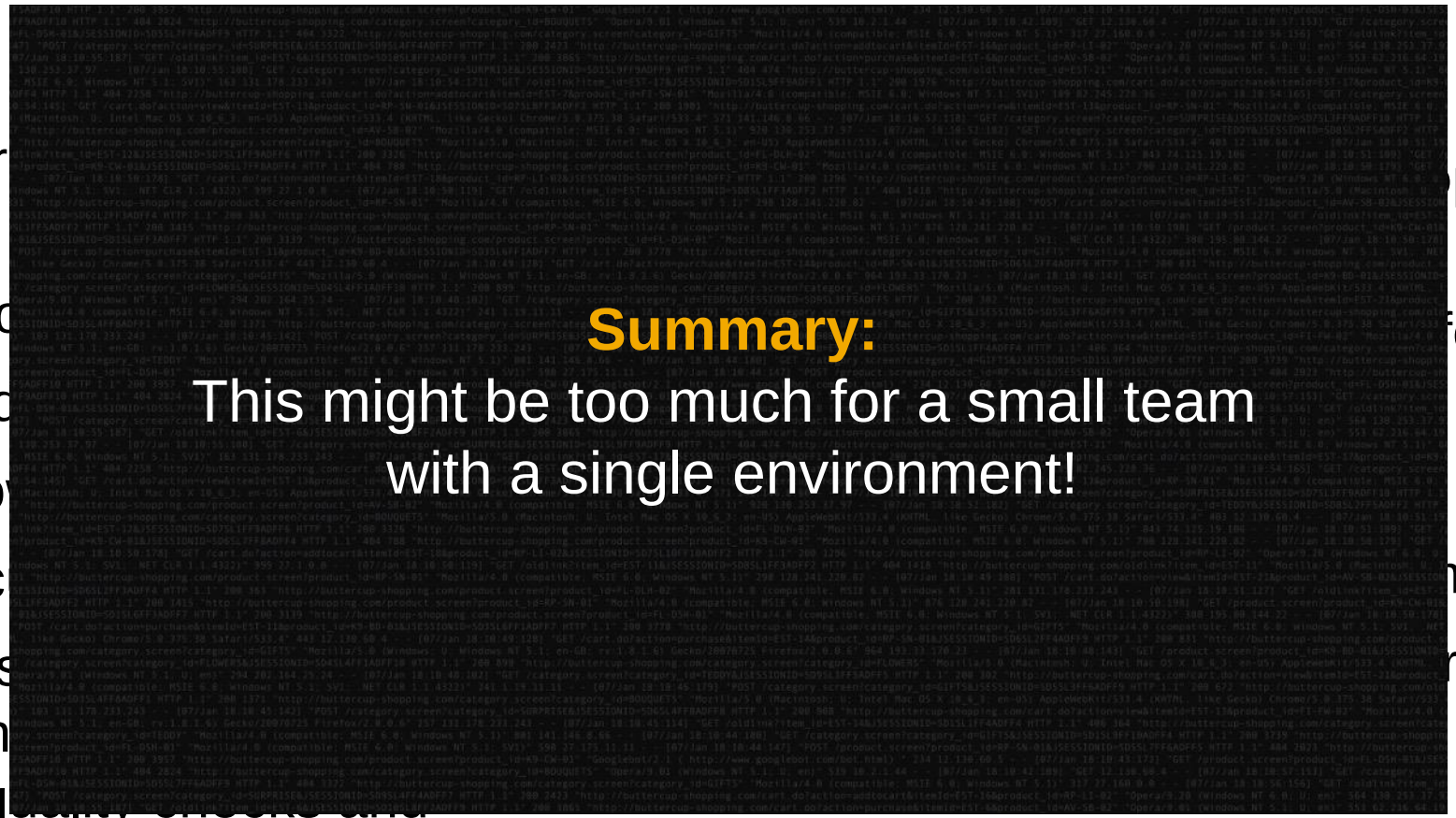


The heavy solution (Cont'd)

Complete control on changes

Advantages

- All configs ar … ps … Lots of traceability
- Multi-team co … for deploying
- Better code c …
- Promote kno …
- Create a sec … naintain
- Off-load the s … rit creation to th … to focus on q … improvement.



Problem: Many ways to effect change

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

- Click in the web UI
- Deploy som
  - deployment
  - cluster mast
  - search head
- Edit conf file
  (and then prob
- `inputlooku`
- Things in KV
- Can you thi

Solution:

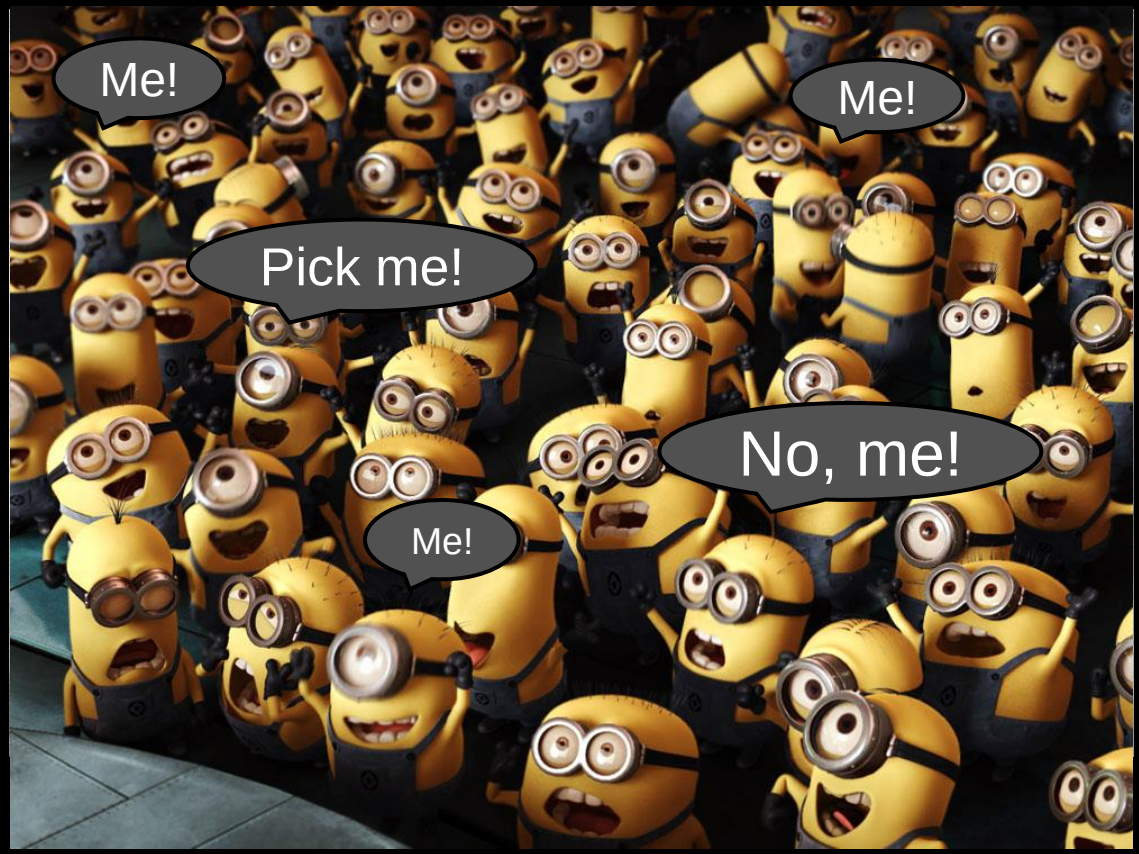
Let it be!

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



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

=

Runtine example.conf

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

Problem: complex precedence rules

How does it apply to Splunk config?

Index time processing

vs

Search time processing

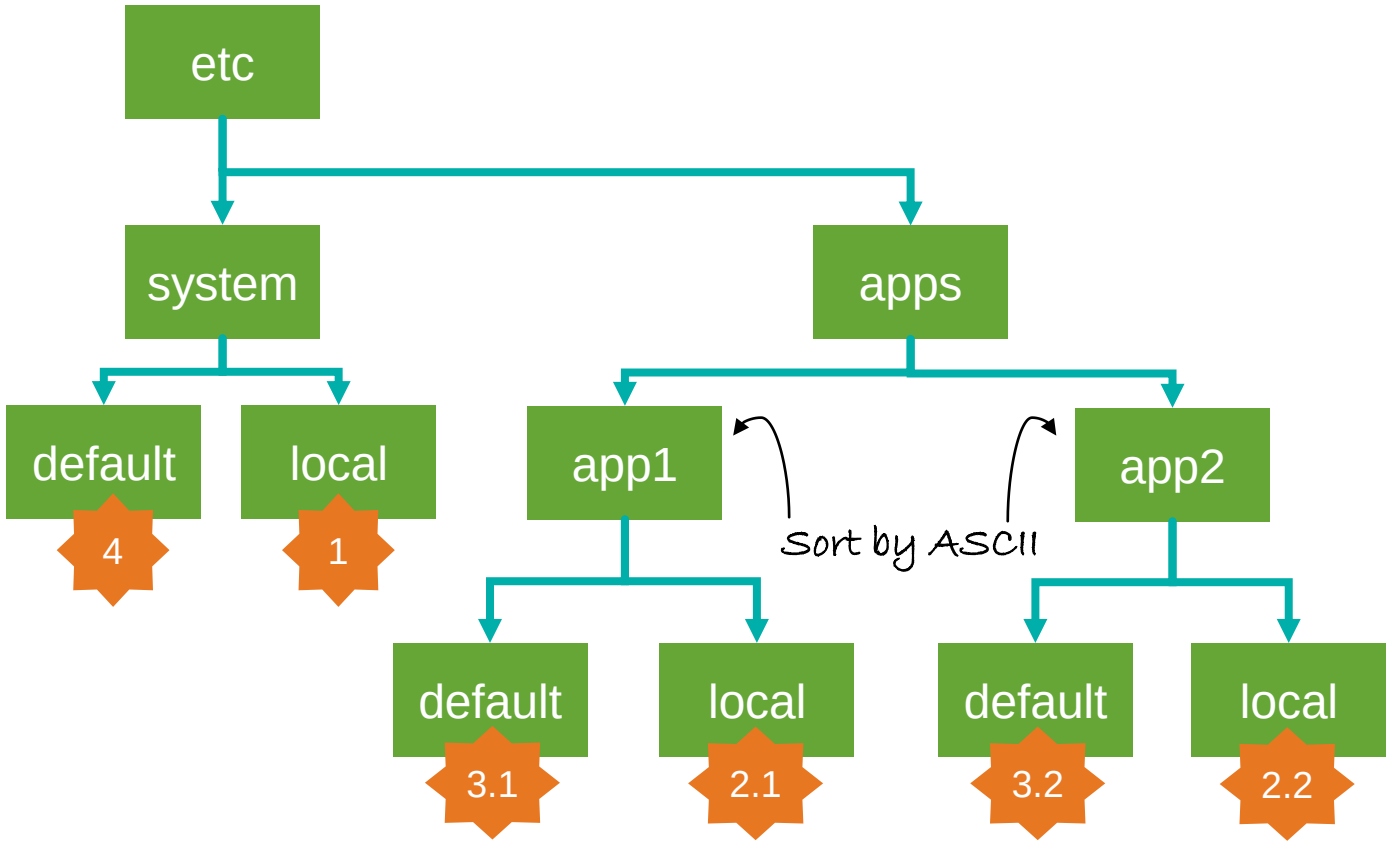
Problem: complex precedence rules

Index time processing : on indexers or forwarders

Indexer cluster

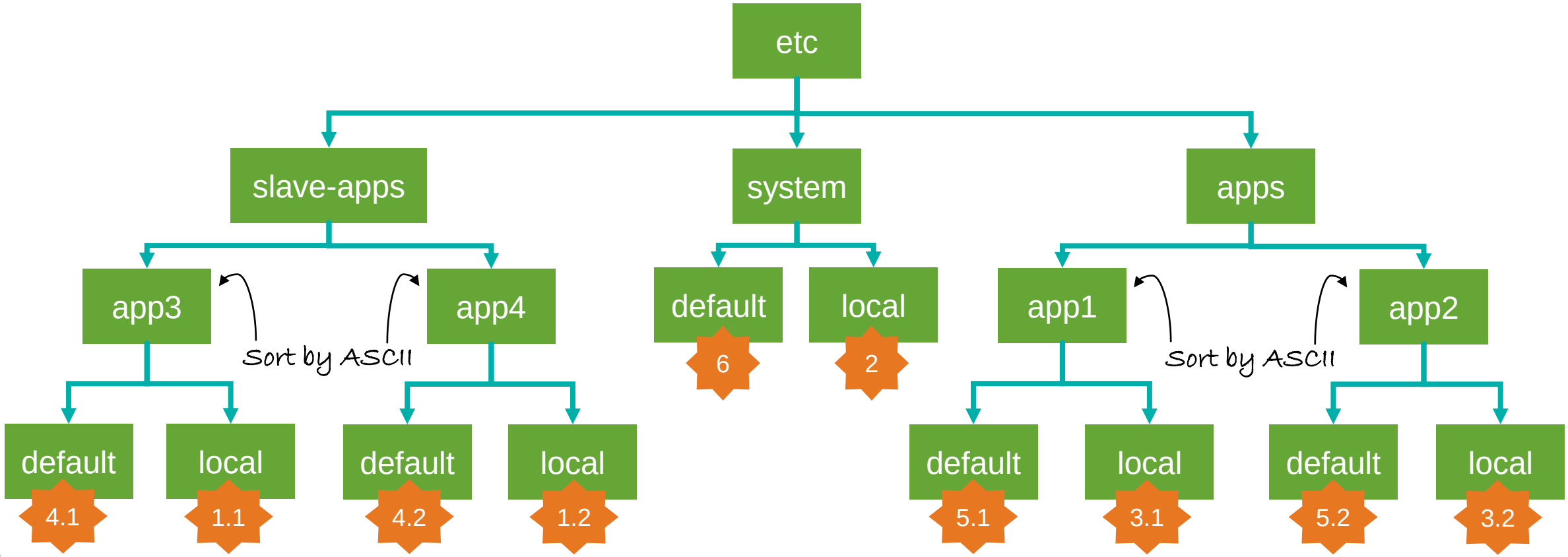
Any impact on precedence rules if you are using indexer cluster?

Answer: YES



Problem: complex precedence rules

Index time processing : on indexers



Problem: complex precedence rules

Search time processing : on search heads

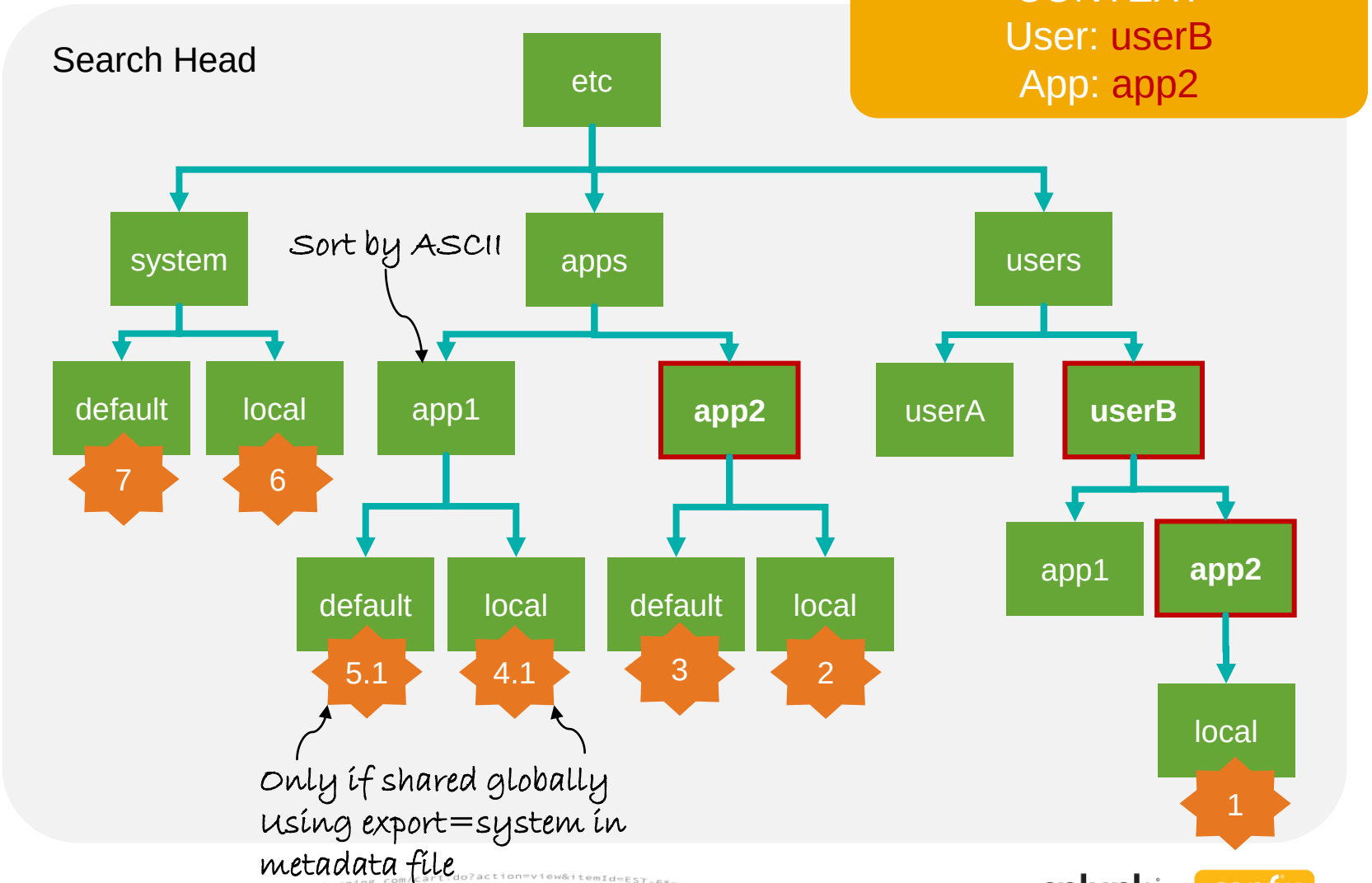
⚠ Beware of ES

"import=app1,app2,…" in metadata overwrites the "export=system"

ⓘ Search head cluster

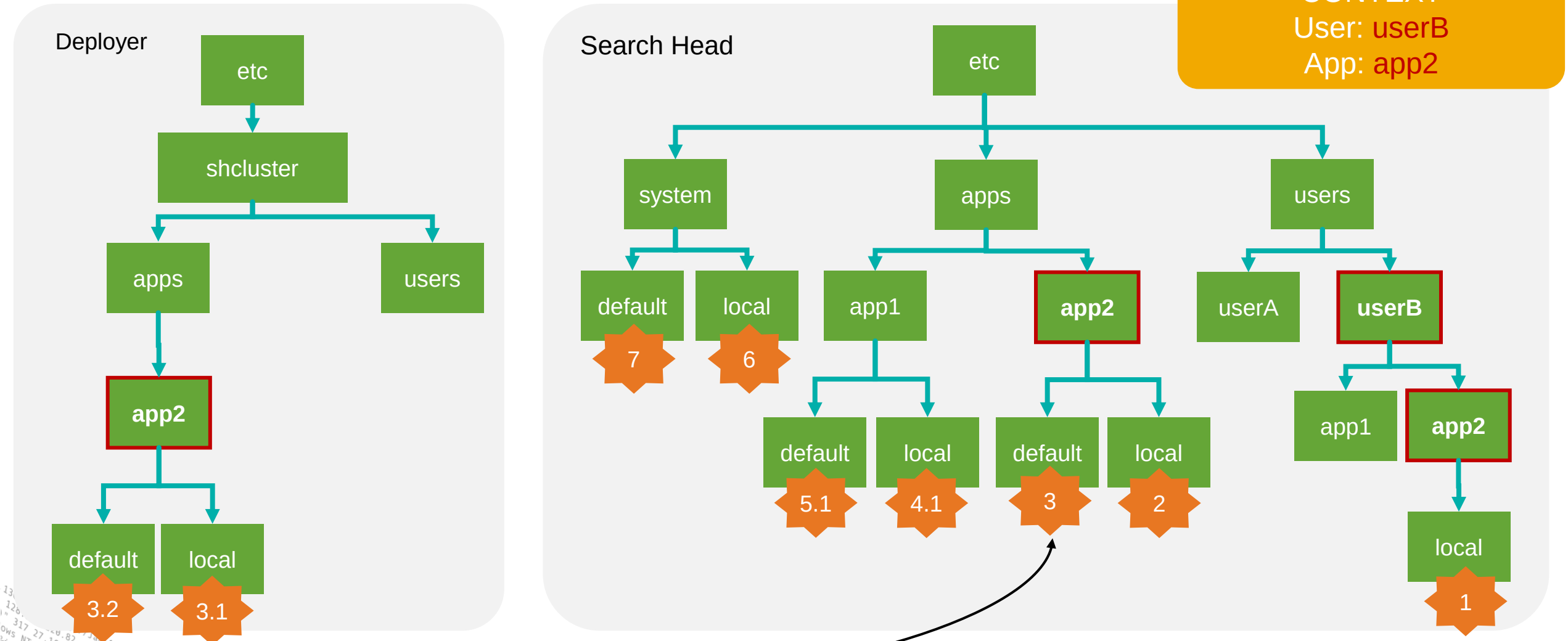
Any impact on precedence rules if you are using search head cluster?

Answer: YES



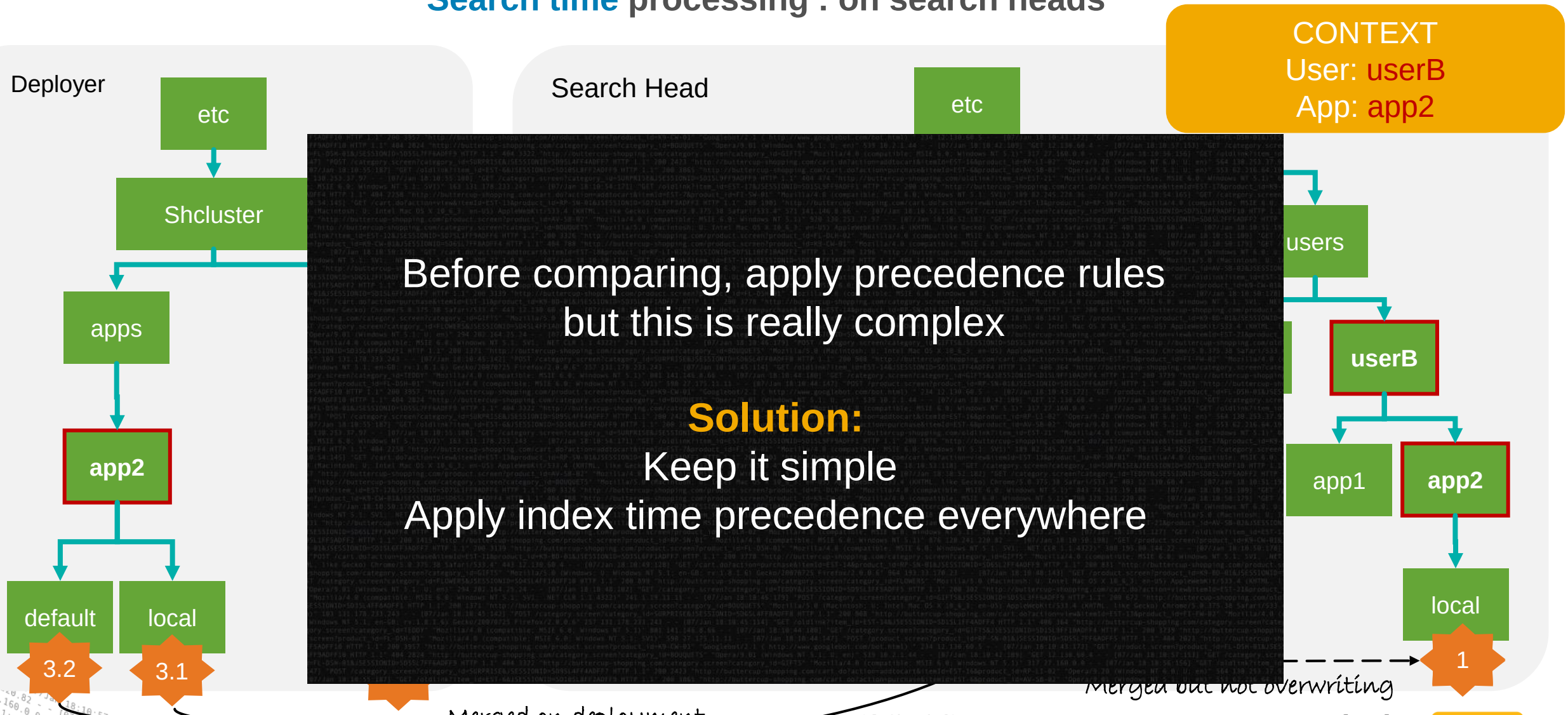
Problem: complex precedence rules

Search time processing : on search heads



Problem: complex precedence rules

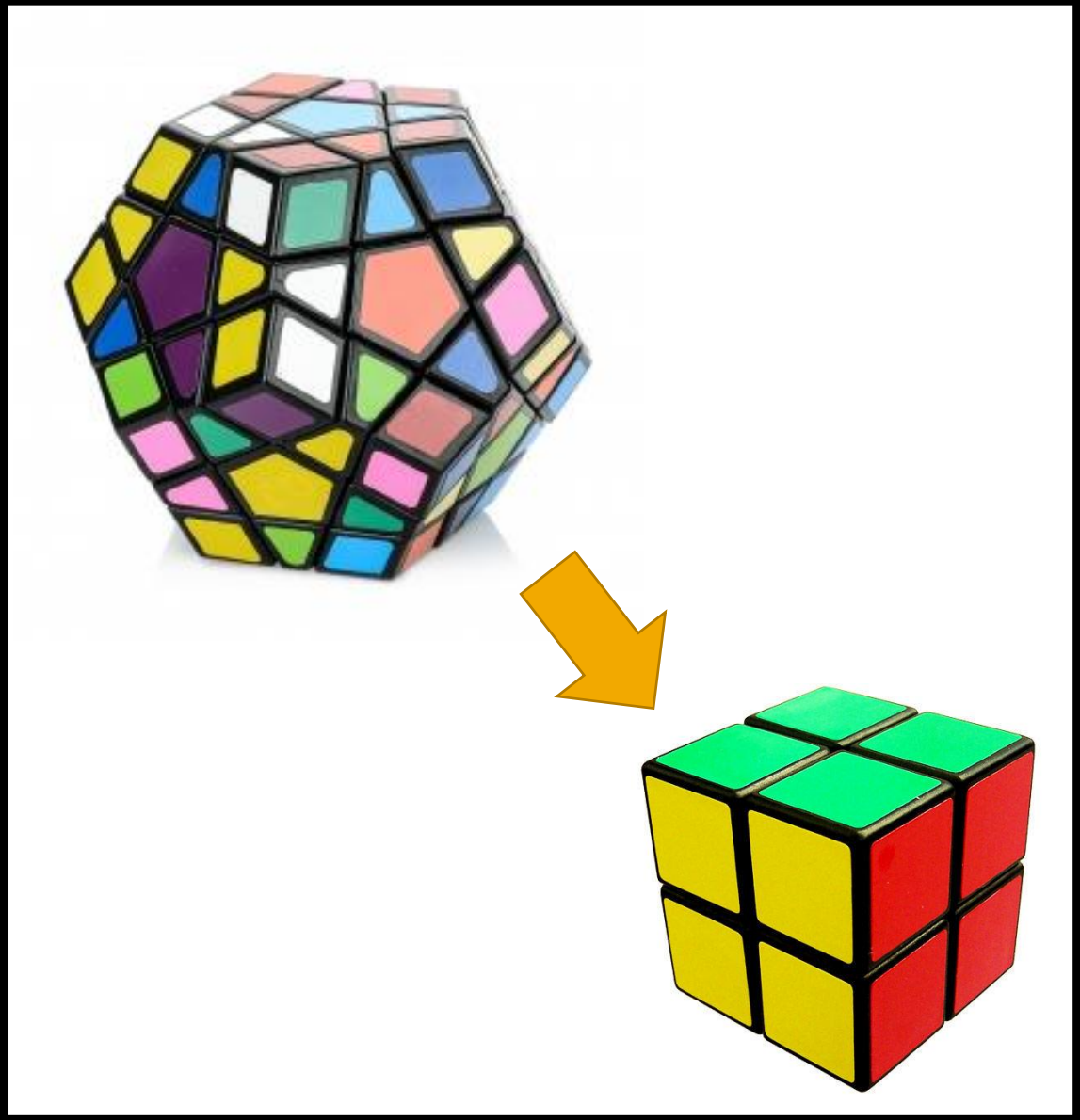
Search time processing : on search heads



splunk> .conf18

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?

Canonicalisation

Splunk instance

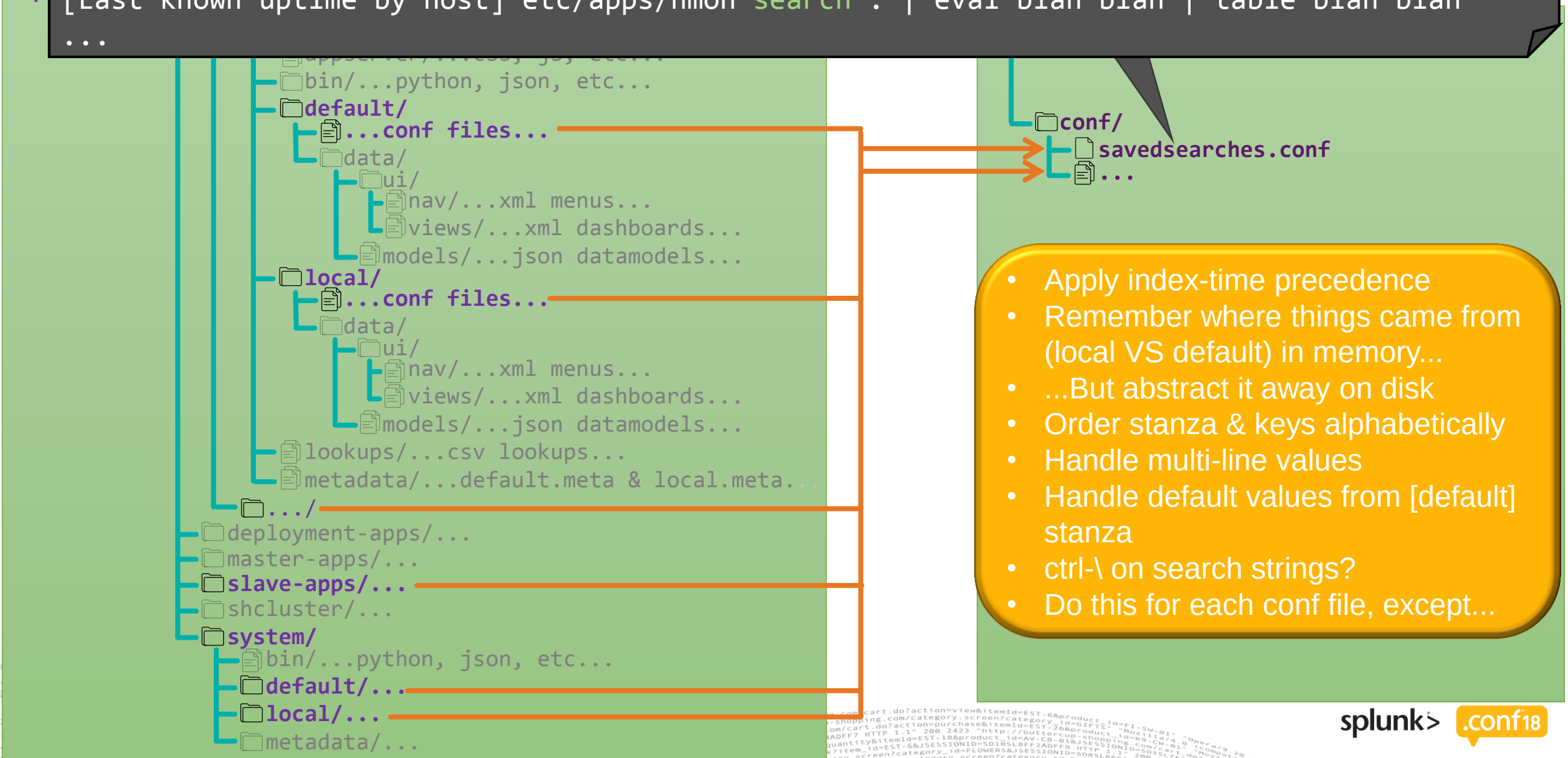
```
/opt/splunk/etc/
    apps/
        myapp/
            appserver/...css, js, etc...
            bin/...python, json, etc...
            default/
                ...conf files...
                data/
                    ui/
                        nav/...xml menus...
                        views/...xml 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/...
```

Only enabled apps!

Canonical version on disk

```
/canonical/
```

```
[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
...
```



- Apply index-time precedence
- Remember where things came from (local VS default) in memory...
- ...But abstract it away on disk
- Order stanza & keys alphabetically
- Handle multi-line values
- Handle default values from [default] stanza
- ctrl-\ on search strings?
- Do this for each conf file, except...

Canonicalisation

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

Splunk instance

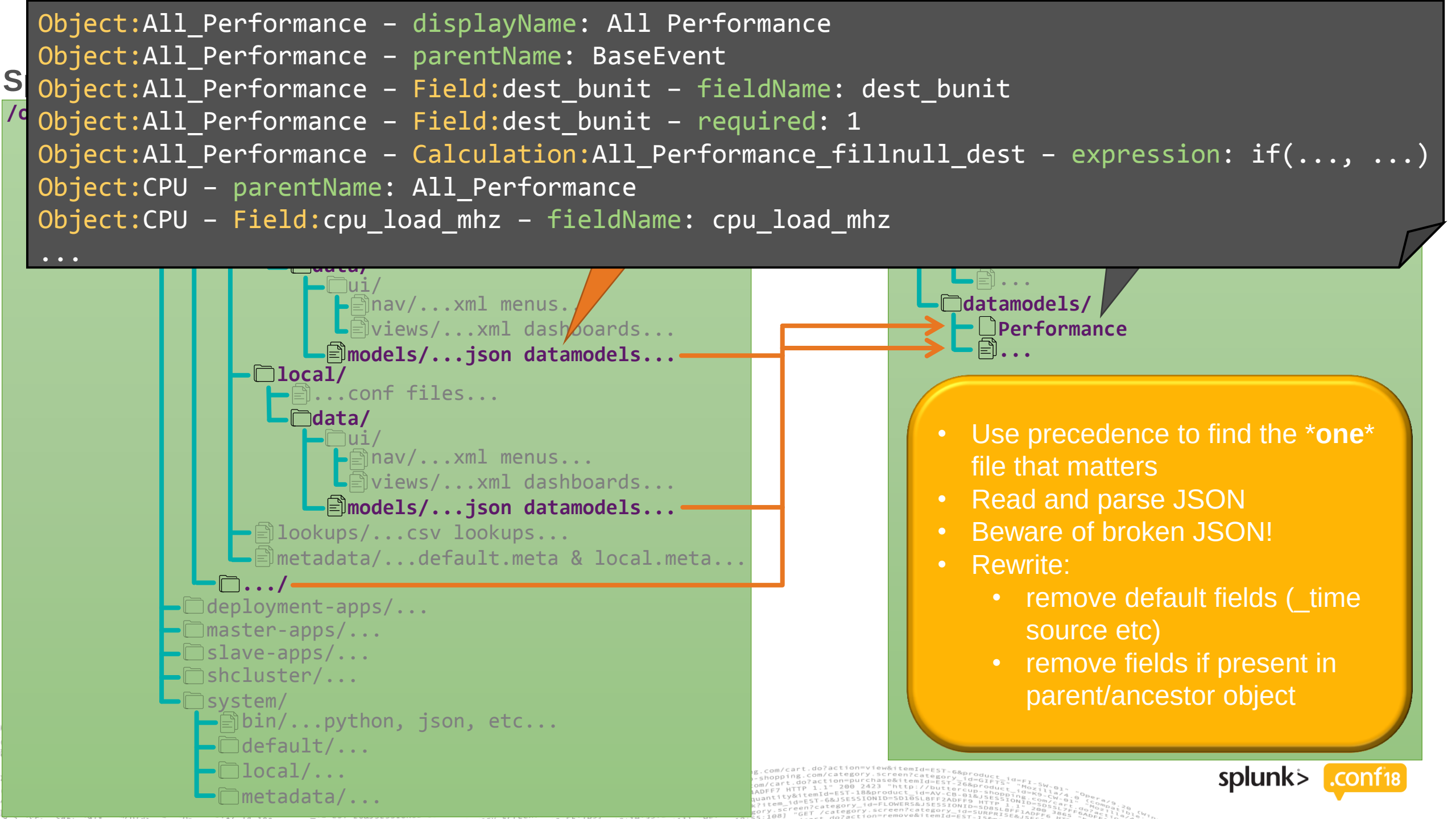
```
/opt/splunk/etc/
    apps/
        myapp/
            appserver/...css, js, etc...
            bin/...python, json, etc...
            default/
                ...conf files...
                data/
                    ui/
                        nav/...xml menus...
                        views/...xml 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/...
```

Canonical version on disk

```
/canonical/
    appconf/
        myapp
        ...
    conf/
        savedsearches.conf
        ...
```

- 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
...
```



- 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> .conf18

Canonicalisation – csv lookups

Splunk instance

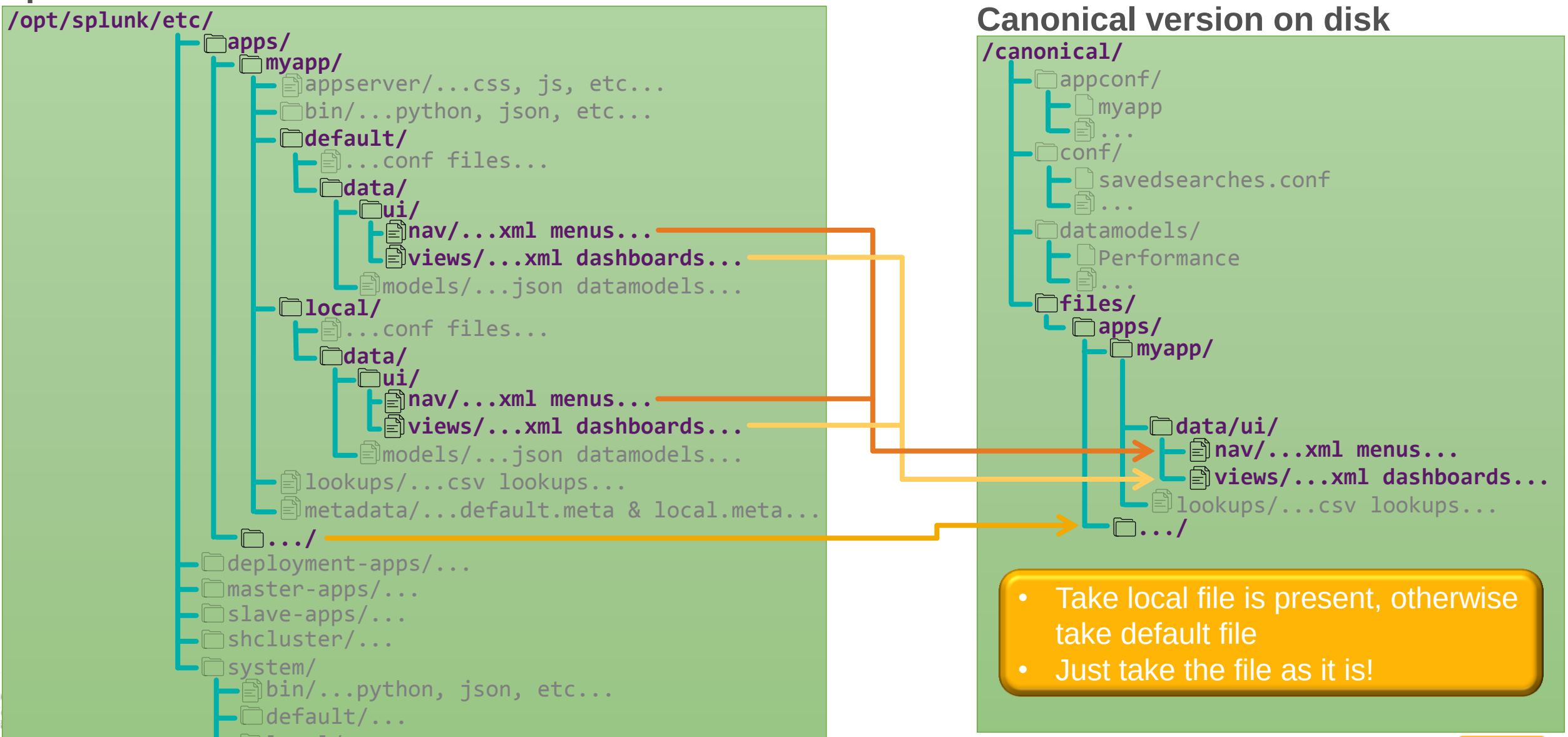
```
/opt/splunk/etc/
    apps/
        myapp/
            appserver/...css, js, etc...
            bin/...python, json, etc...
            default/
                ...conf files...
                data/
                    ui/
                        nav/...xml menus...
                        views/...xml 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/...
```

Canonical version on disk

```
/canonical/
    appconf/
        myapp
        ...
    conf/
        savedsearches.conf
        ...
    datamodels/
        Performance
        ...
    files/
        apps/
            myapp/
                lookups/...csv lookups...
                .../
```

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

Canonicalisation – other local/default



splunk> .conf18

Canonicalisation – anything else

Splunk instance

/opt/splunk/etc/

- apps/
  - myapp/
    - appserver/...css, js, etc...
    - bin/...python, json, etc...
    - default/
      - ...conf files...
      - 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/...

apps/splunk_app_microsoft_exchange/bin/TimeBombStatus.json

```
1  -{"status": 401, "message": "Client is not authenticated"}
1  +{"message": "Client is not authenticated", "status": 401}
```

Canonical version on disk

/canonical/

- appconf/
  - myapp
  - ...
- conf/
  - ...es.conf
  - ...
- files/
  - apps/
    - myapp/
      - appserver/...css, js, etc...
      - bin/...python, json, etc...
      - data/ui/
        - nav/...xml menus...
        - views/...xml dashboards...
      - lookups/...csv lookups...
    - .../
  - system/
    - bin/...python, json, etc...
    - ...
  - ...

- No precedence
- Copy as is, except json

Canonicalisation – metadata

Splunk instance

/opt/splunk/etc/

- apps/
  - myapp/
    - appserver/...css, js, etc...
    - bin/...python, json, etc...
    - default/
      - ...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/...**

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

Canonical version on disk

/canonical/

- appconf/
  - myapp
  - ...
- conf/
  - savedsearches.conf
  - ...
- datamodels/
- f
- ...
- meta/
  - myapp
  - ...

- 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)

splunk> .conf18

Canonicalisation

Splunk instance

```
/opt/splunk/etc/
    apps/
        myapp/
            appserver/...css, js, etc...
            bin/...python, json, etc...
            default/
                ...conf files...
                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/...
```

Canonical version on disk

```
/canonical/
    appconf/
        myapp
        ...
    conf/
        savedsearches.conf
        ...
    datamodels/
        Performance
        ...
    files/
        apps/
            myapp/
                appserver/...css, js, etc...
                bin/...python, json, etc...
                data/ui/
                    nav/...xml menus...
                    views/...xml dashboards...
                lookups/...csv lookups...
            .../
        system/
            bin/...python, json, etc...
            ...
        ...
    meta/
        myapp
        ...
```

splunk> .conf18

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 -

Time Range

Earliest Time:

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

Latest Time: +0s

Type a latest time using relative time modifiers.

Cron Schedule *: 4 0 * * 6

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

splunk> .conf18

explosion 1: conf stanza

etc/apps/SA-AccessProtection/local/savedsearches.conf — View file @ 462526ed

```
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   1   [Access - Insecure Or Cleartext Authentication - Rule]
9   2   action.customsearchbuilder.enabled = true
10  3   action.nbtstat.param.verbose = 0
... ... @@ -92,3 +85,19 @@ realtime_schedule = 0
92  85  relation = greater than
93  86  schedule_window = auto
94  87  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 = false
    91  + action.nbtstat.param.verbose = 0
    92  + action.nslookup.param.verbose = 0
    93  + action.ping.param.verbose = 0
    94  + cron_schedule = 4 0 * * 6
    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
```

splunk> .conf18

~~explosion~~ 1: conf stanza

btool_savedsearches — View file @ 2a66d914

```
...  ...  @@ -5710,6 +5710,7 @@ vsid =
5710 5710  action.correlationsearch = 0
5711 5711  action.correlationsearch.enabled = 1
5712 5712  action.correlationsearch.label = Completely Inactive Account
     5713 + action.customsearchbuilder.enabled = false
5713 5714  action.email = 1
5714 5715  action.email.format = csv
5715 5716  action.email.inline = 1
...  ...  @@ -5767,7 +5768,7 @@ auto_summarize.max_time = 3600
5767 5768  auto_summarize.suspend_period = 24h
5768 5769  auto_summarize.timespan =
5769 5770  counttype = number of events
5770      - cron_schedule = 3 0 * * 6
     5771 + cron_schedule = 4 0 * * 6
5771 5772  description = Accounts that are no longer used.
5772 5773  disabled = 0
5773 5774  dispatch.auto_cancel = 0
...  ...  @@ -5862,13 +5863,13 @@ display.visualizations.custom.sankey_diagram_app.sankey_diagram.colorMode = cate
5862 5863  display.visualizations.custom.sankey_diagram_app.sankey_diagram.maxColor = #3fc77a
5863 5864  display.visualizations.custom.sankey_diagram_app.sankey_diagram.minColor = #d93f3c
5864 5865  display.visualizations.custom.sankey_diagram_app.sankey_diagram.numOfBins = 6
5865      - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showBackwards = false
5866      - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLabels = true
5867      - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLegend = true
5868      - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showSelf = false
5869      - display.visualizations.custom.sankey_diagram_app.sankey_diagram.showTooltip = true
5870      - display.visualizations.custom.sankey_diagram_app.sankey_diagram.styleBackwards = false
5871      - display.visualizations.custom.sankey_diagram_app.sankey_diagram.useColors = true
     5866 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showBackwards = 0
     5867 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLabels = 1
     5868 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLegend = 1
     5869 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showSelf = 0
     5870 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.showTooltip = 1
     5871 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.styleBackwards = 0
     5872 + display.visualizations.custom.sankey_diagram_app.sankey_diagram.useColors = 1
5872 5873  display.visualizations.custom.timeline_app.timeline.axisTimeFormat = SECONDS
```

```
> splunk btool savedsearches list
```

? which search?

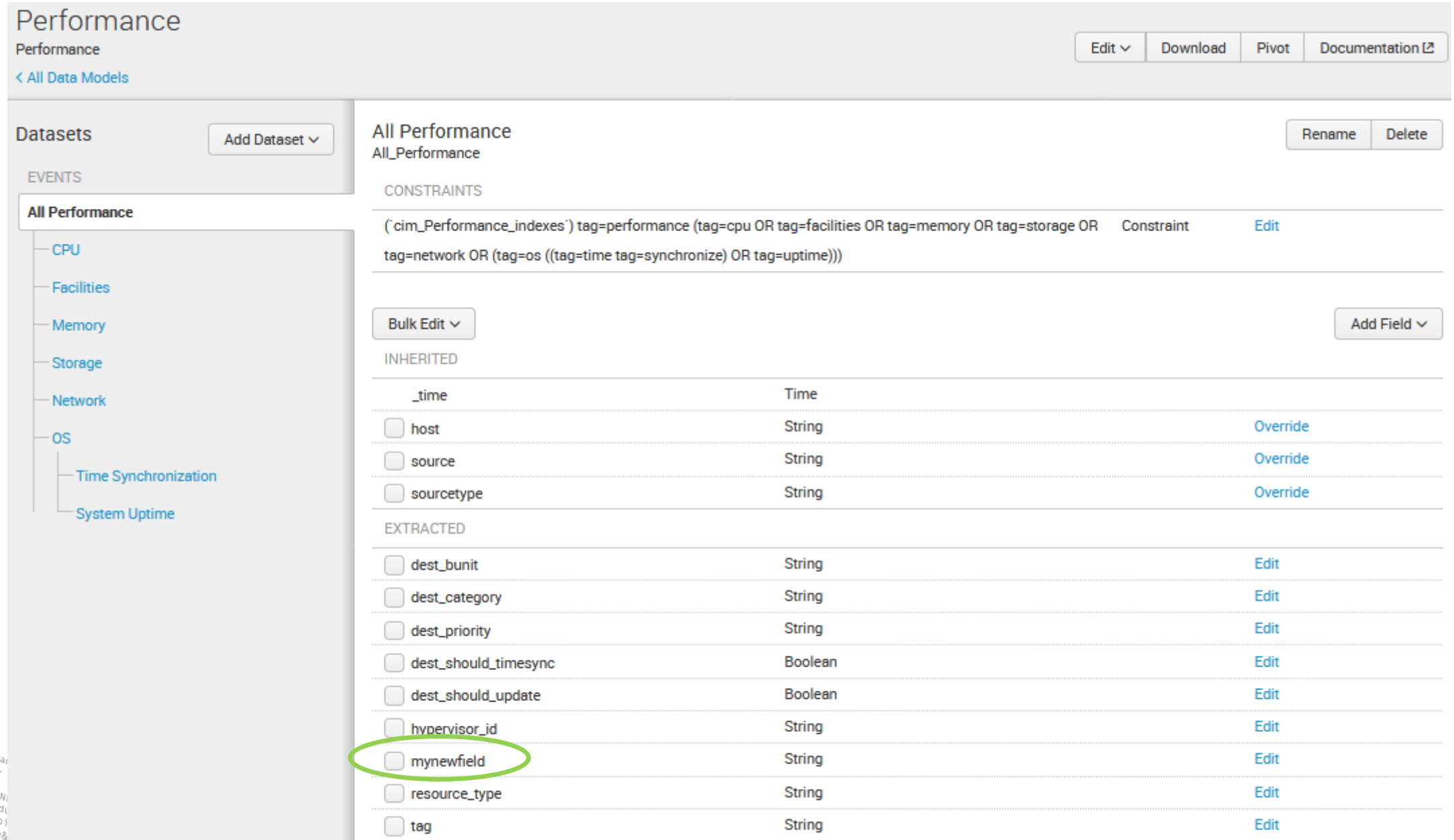
~~explosion~~ 1: conf stanza

conf/savedsearches.conf — View file @ d942911a

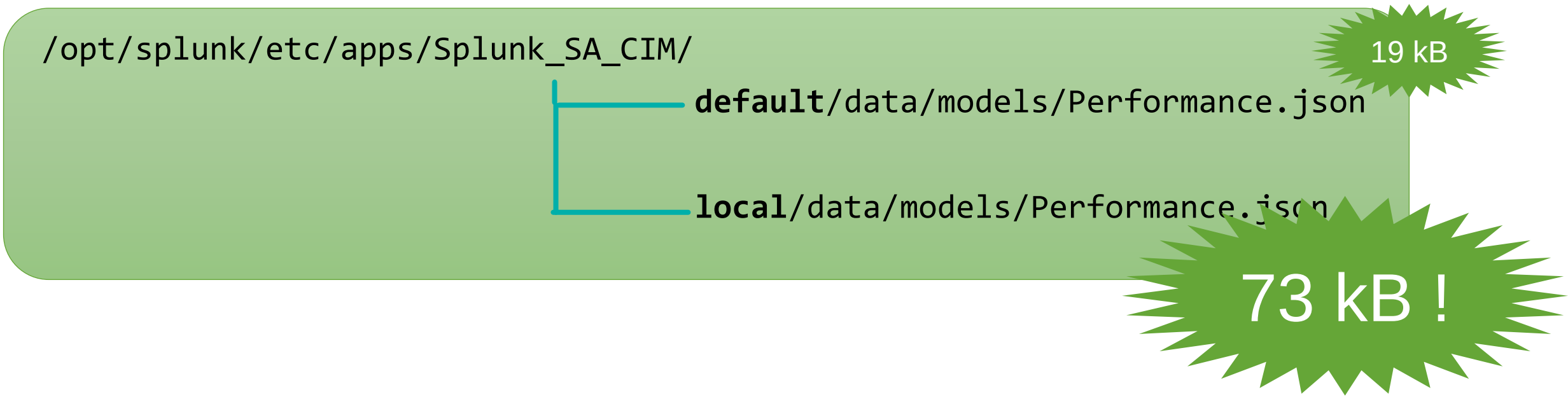
```
...  ...  @@ -5684,6 +5684,7 @@
5684 5684 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.correlationsearch.enabled = 1
5685 5685 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.correlationsearch.label =
5686 5686 Completely Inactive Account
     5687 + [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.customsearchbuilder.enabled = false
5687 5688 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.email = 1
5688 5689 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.email.format = csv
5689 5690 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection action.email.inline = 1
...  ...  @@ -5741,7 +5742,7 @@
5741 5742 [Access - Completely Inactive Account - Rule] etc/system auto_summarize.suspend_period = 24h
5742 5743 [Access - Completely Inactive Account - Rule] etc/system auto_summarize.timespan =
5743 5744 [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
5745 5746 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection description = Accounts that are no longer
5746 5747 used.
5747 5748 [Access - Completely Inactive Account - Rule] etc/apps/SA-AccessProtection disabled = 0
5748 5749 [Access - Completely Inactive Account - Rule] etc/system dispatch.auto_cancel = 0
...  ...  @@ -5836,13 +5837,13 @@
5836 5837 [Access - Completely Inactive Account - Rule] etc/apps/sankey_diagram_app
display.visualizations.custom.sankey_diagram_app.sankey_diagram.maxColor = #3fc77a
5837 5838 [Access - Completely Inactive Account - Rule] etc/apps/sankey_diagram_app
display.visualizations.custom.sankey_diagram_app.sankey_diagram.minColor = #d93f3c
5838 5839 [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
5840      - [Access - Completely Inactive Account - Rule] etc/system
display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLabels = true
5841      - [Access - Completely Inactive Account - Rule] etc/system
display.visualizations.custom.sankey_diagram_app.sankey_diagram.showLegend = true
5842      - [Access - Completely Inactive Account - Rule] etc/system
display.visualizations.custom.sankey_diagram_app.sankey_diagram.showSelf = false
5843      - [Access - Completely Inactive Account - Rule] etc/system
display.visualizations.custom.sankey_diagram_app.sankey_diagram.showTooltip = true
5844      - [Access - Completely Inactive Account - Rule] etc/system
display.visualizations.custom.sankey_diagram_app.sankey_diagram.styleBackwards = false
5845      - [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
```

splunk> .conf18

Explosion 2: Data model definition



Explosion 2: Data model definition



Explosion 2: Data model definition

```
                "required": false,
                "multivalue": false,
-                               "hidden":               false
            },
            {
-                               "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},
                "fieldName": "tag",
-                               "displayName":  "tag",
                "type": "string",
                "fieldSearch": "",
                "required": false,
                "multivalue": true,
-                               "hidden":               false
```

```
                "required": false,
                "multivalue": false,
+               "hidden": false,
+               "editable": true,
+               "displayName": "resource_type",
+               "comment": ""
            },
            {
                "fieldName": "tag",
+               "owner": "All_Performance",
                "type": "string",
                "fieldSearch": "",
                "required": false,
                "multivalue": true,
+               "hidden": false,
+               "editable": true,
+               "displayName": "tag",
+               "comment": ""
+           },
+           {
+               "fieldName": "mynewfield",
+               "owner": "All_Performance",
+               "type": "string",
+               "fieldSearch": "",
+               "required": false,
+               "multivalue": false,
+               "hidden": false,
+               "editable": true,
+               "displayName": "mynewfield",
+               "comment": ""
+           },
+           {
+               "fieldName": "_time",
+               "owner": "BaseEvent",
+               "type": "timestamp",
+               "fieldSearch": "",
+               "required": false,
+               "multivalue": false,
+               "hidden": false,
+               "editable": true,
+               "displayName": "_time",
```

Explosion 2: Data model definition

Performance

Performance

< All Data Models

Edit | Download | Pivot | Documentation

Datasets | Add Dataset

EVENTS

All Performance

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

Rename | Delete

straint 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

datamodels/Performance — View file @ 98f1b781

```
@@ -42,6 +42,12 @@ DM:Performance - Object:All_Performance - Field:hypervisor_id - type: string
 DM:Performance - Object:All_Performance - Field:hypervisor_id - required: 1
 DM:Performance - Object:All_Performance - Field:hypervisor_id - hidden: 1
 DM:Performance - Object:All_Performance - Field:hypervisor_id - multivalue: 1
+DM:Performance - Object:All_Performance - Field:mynewfield - fieldName: mynewfield
+DM:Performance - Object:All_Performance - Field:mynewfield - displayName: mynewfield
+DM:Performance - Object:All_Performance - Field:mynewfield - type: string
+DM:Performance - Object:All_Performance - Field:mynewfield - required: 1
+DM:Performance - Object:All_Performance - Field:mynewfield - hidden: 1
+DM:Performance - Object:All_Performance - Field:mynewfield - multivalue: 1
 DM:Performance - Object:All_Performance - Field:resource_type - fieldName: resource_type
 DM:Performance - Object:All_Performance - Field:resource_type - displayName: resource_type
 DM:Performance - Object:All_Performance - Field:resource_type - type: string
```

splunk> .conf18

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!
```

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

Today

✓ 4 results (20/07/2018 00:00:00.000 to 20/07/2018 09:28:58.000) No Event Sampling Job Verbose Mode

Events | Patterns | Statistics (4) | Visualization

100 Per Page Format Preview

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

splunk> .conf18

Explosion 3: csv lookup

lookups/just_for_fun.csv

```
- zzz,aaa
- hello,bonjour
- hi,au revoir
- hello world,bonjour tout le monde
- hello world!,bonjour tout le monde!
```

```
+ aaa,zzz
+ bonjour,hello
+ "au revoir",goodbye
+ "bonjour tout le monde","hello world"
+ "bonjour tout le monde!","hello world!"
```

~~Explosion~~ 3: csv lookup

just_for_fun.csv — View file @ 206f3cc1

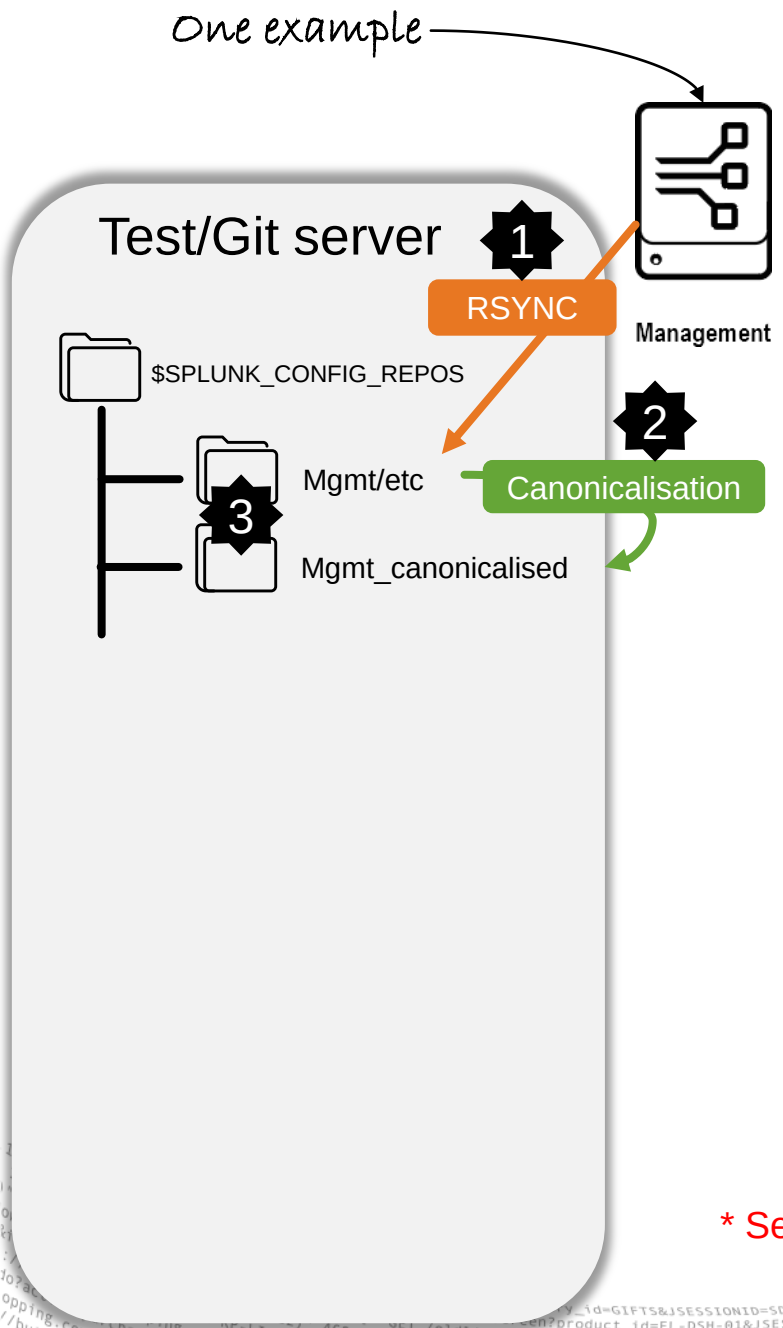
1	aaa,zzz	1	aaa,zzz
2	bonjour,hello	2	bonjour,hello
3	- "au revoir",hi	3	+ "au revoir",goodbye
4	"bonjour tout le monde","hello world"	4	"bonjour tout le monde","hello world"
5	"bonjour tout le monde!","hello world!"	5	"bonjour tout le monde!","hello world!"

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

Change tracking

(not change control)



Change tracking

One server to GIT them all

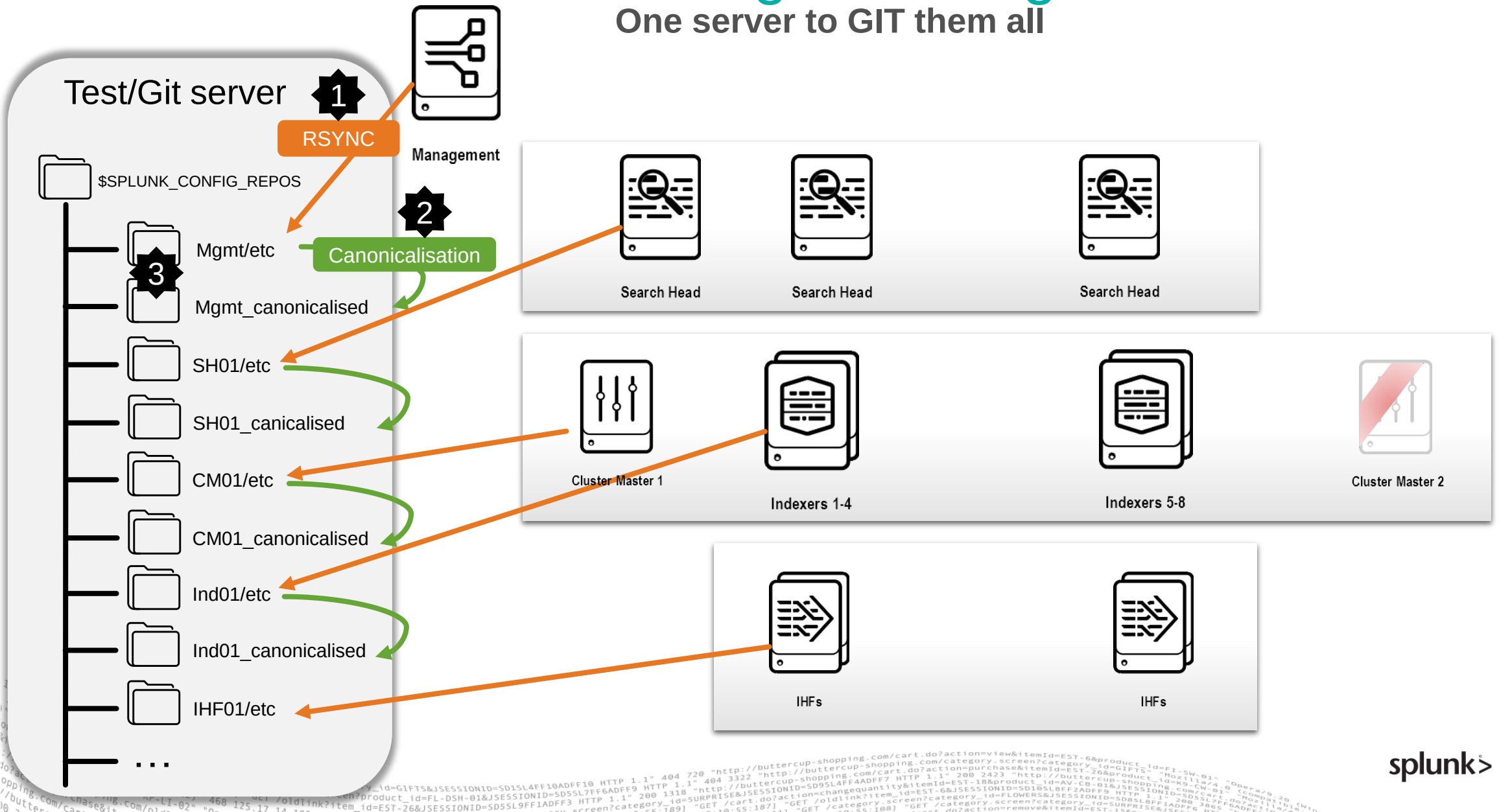
- Rsync $SPLUNK_HOME/etc
  - Exclude some files/folders* such as
    - Large csv files
    - Binaries or jars
    - Some folders: learned app or private object
- Canonicalise “Mgmt/etc” to “Mgmt_canonicalised”
- “Git” both folders
  - Beware of deleted files*

* See bonus slide

splunk> .conf18

Change tracking

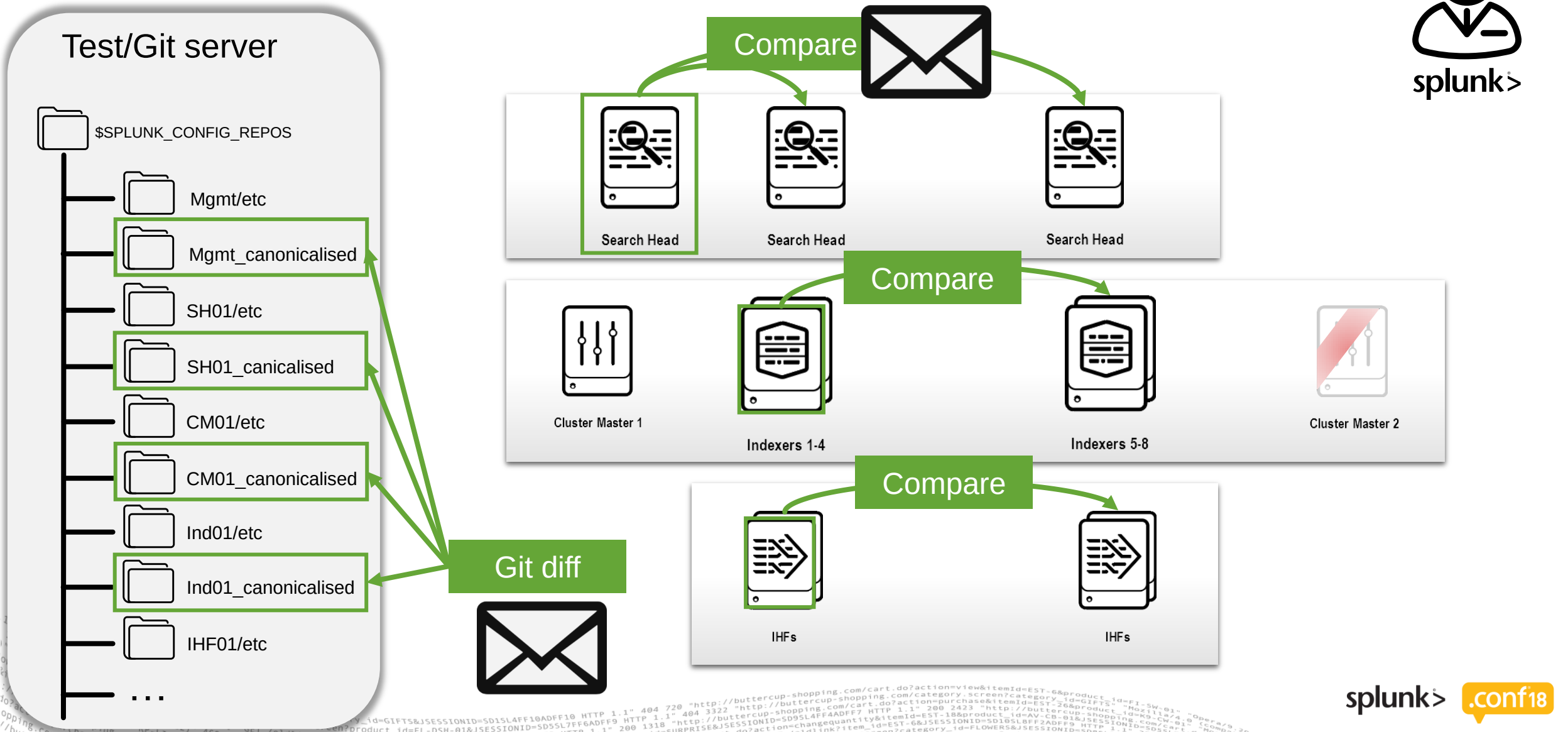
One server to GIT them all



splunk> .conf18

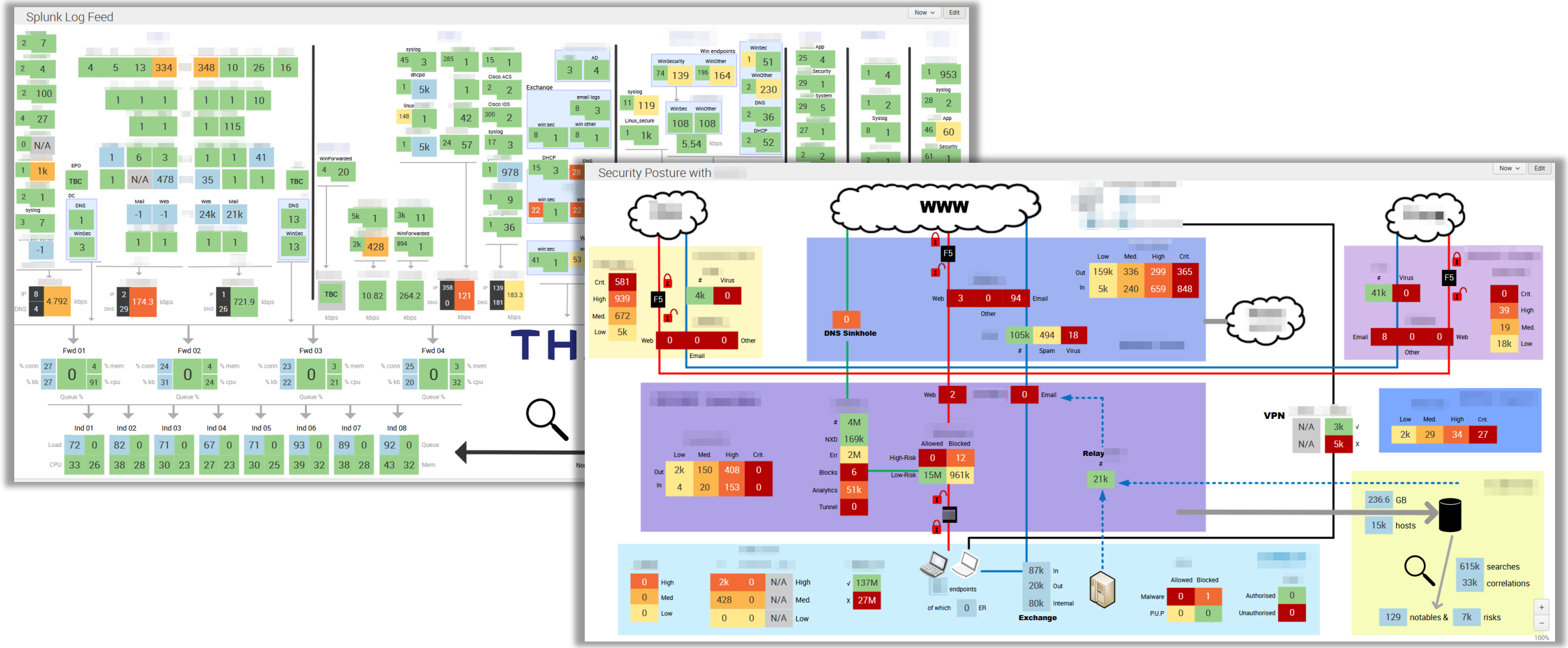
Change tracking

One server to GIT them all



Glass tables

But have you forgotten your glasstables?

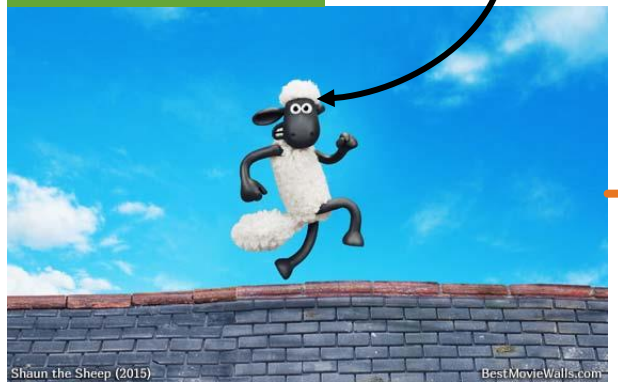


Glass tables

Where are they stored?

Here is one of my glasstables

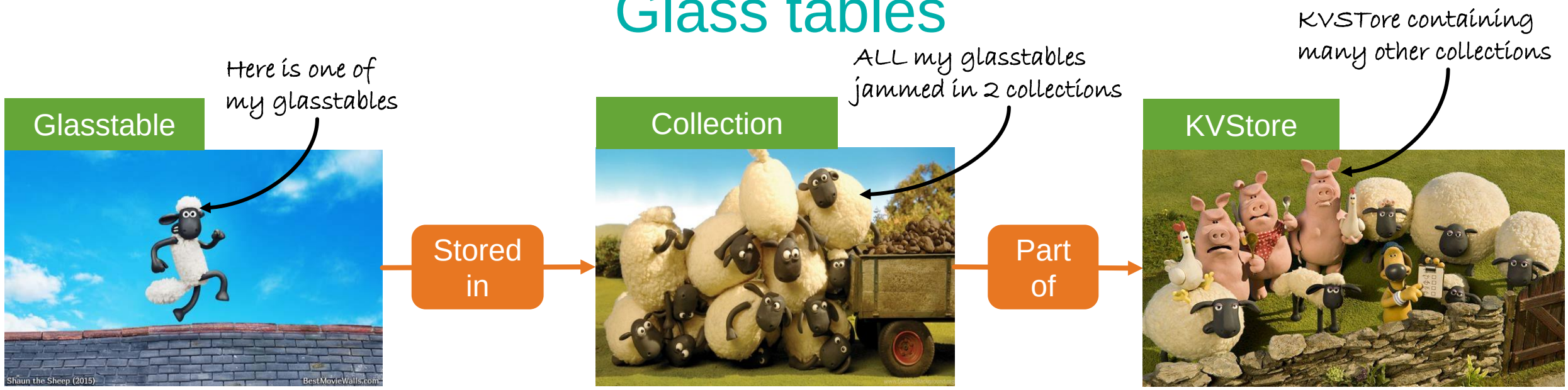
Glasstable



Stored in

~~Glasstables.conf~~

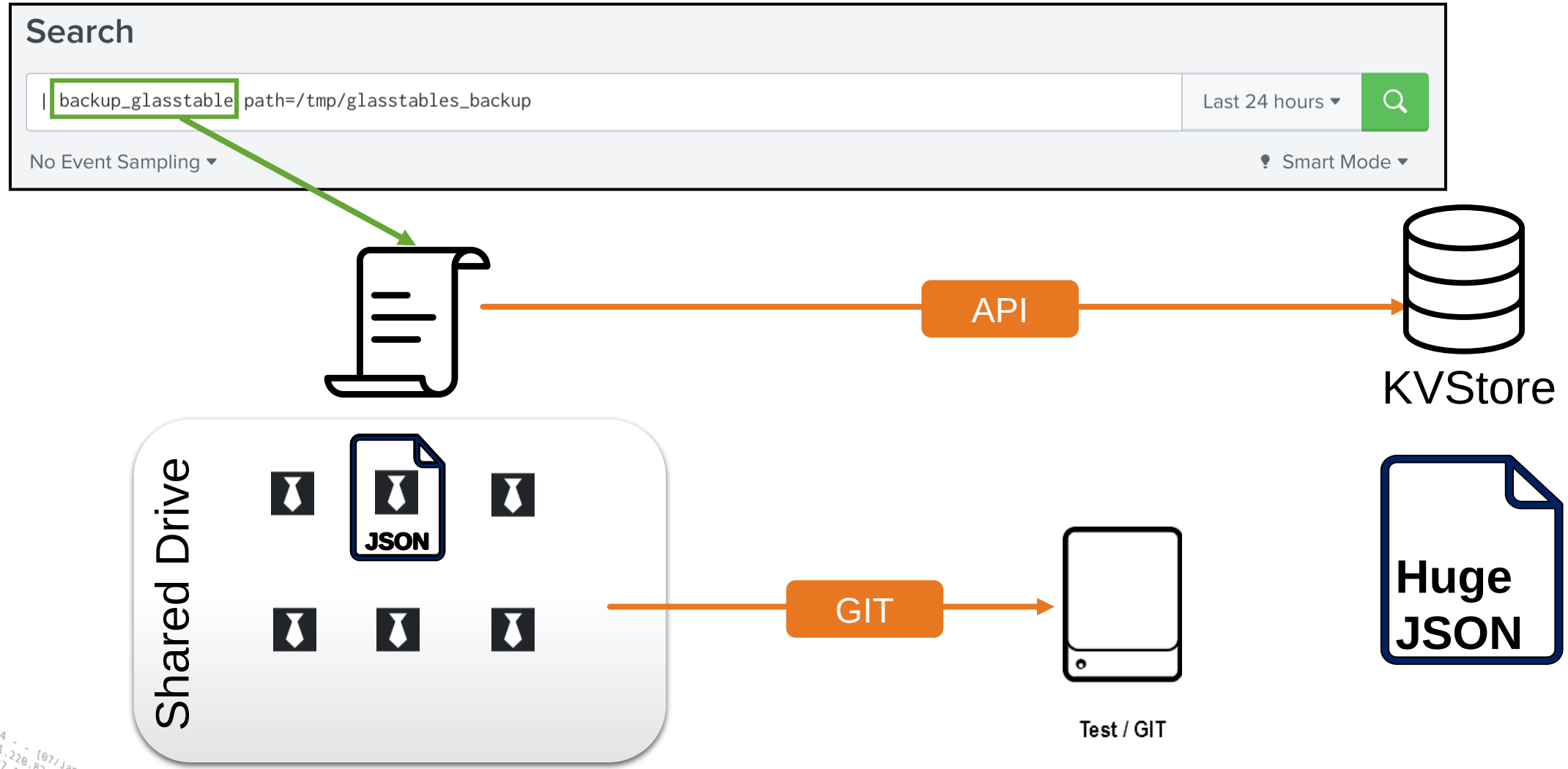
Glass tables



- 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

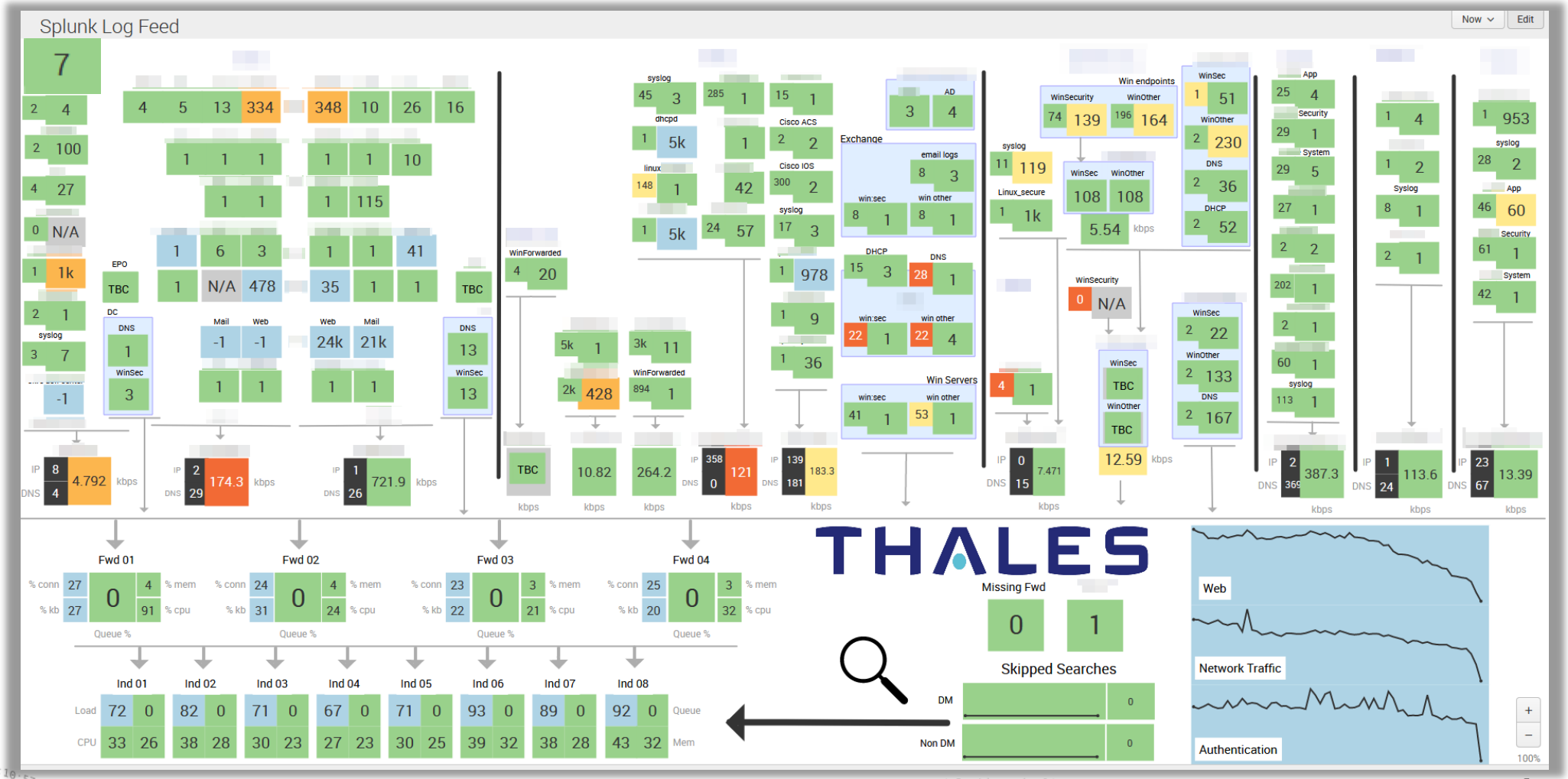
Glass tables

Our tracking/backup solution



Glass tables

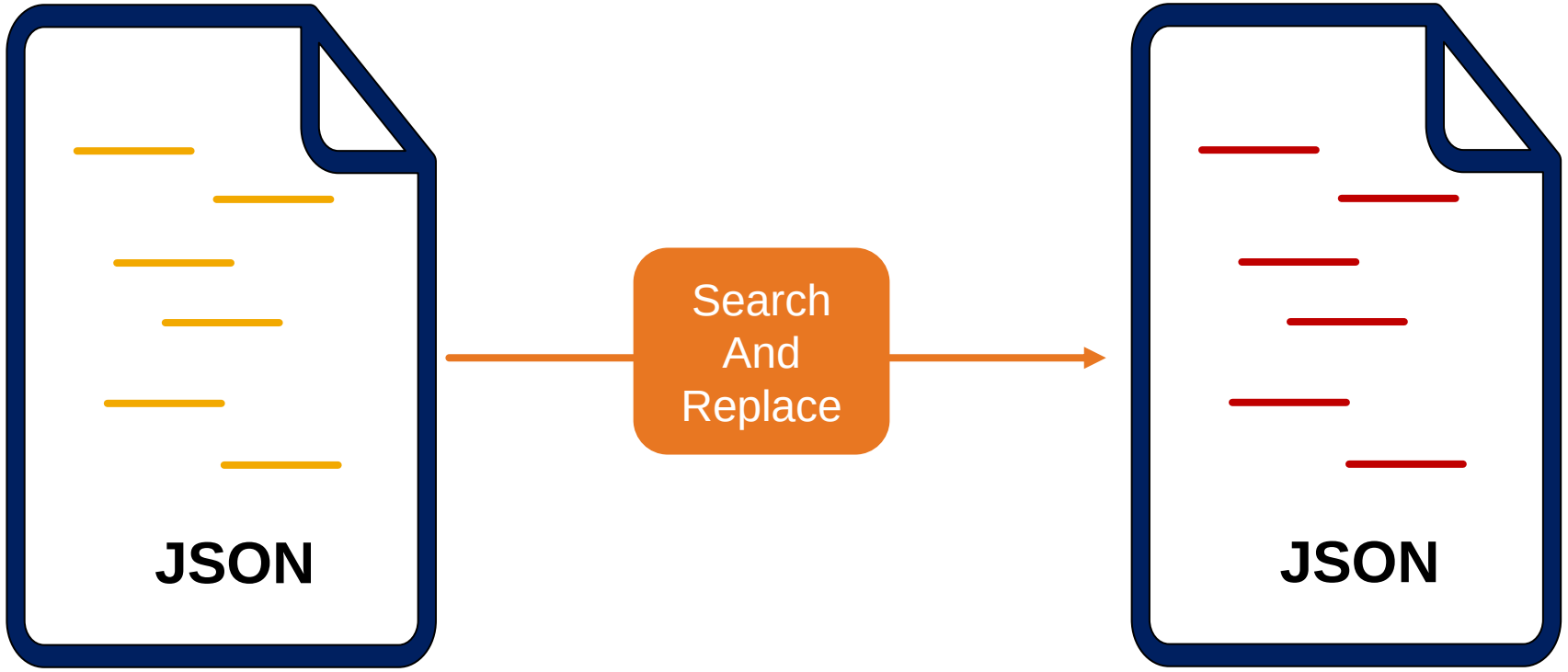
Tracking solution side effect



Glass tables

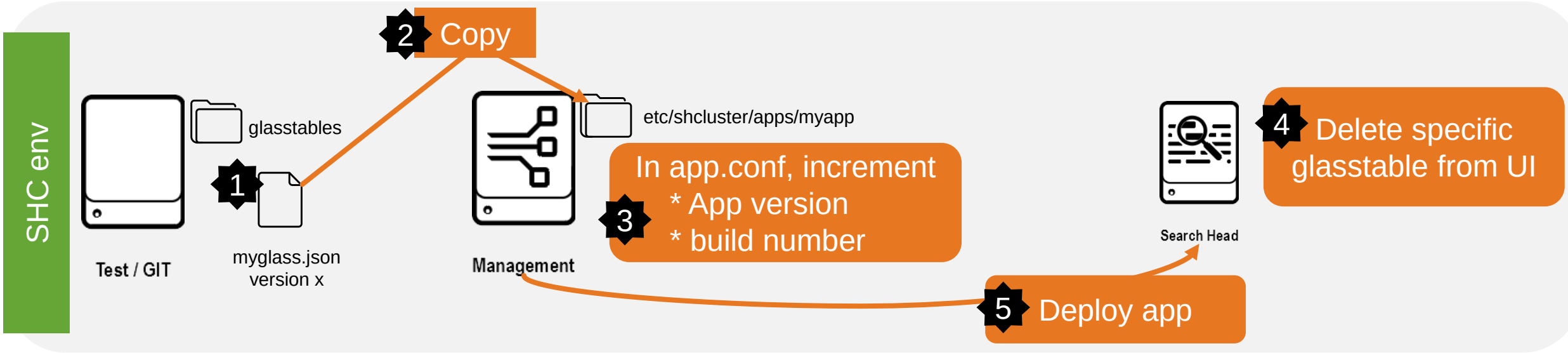
Tracking solution side effect

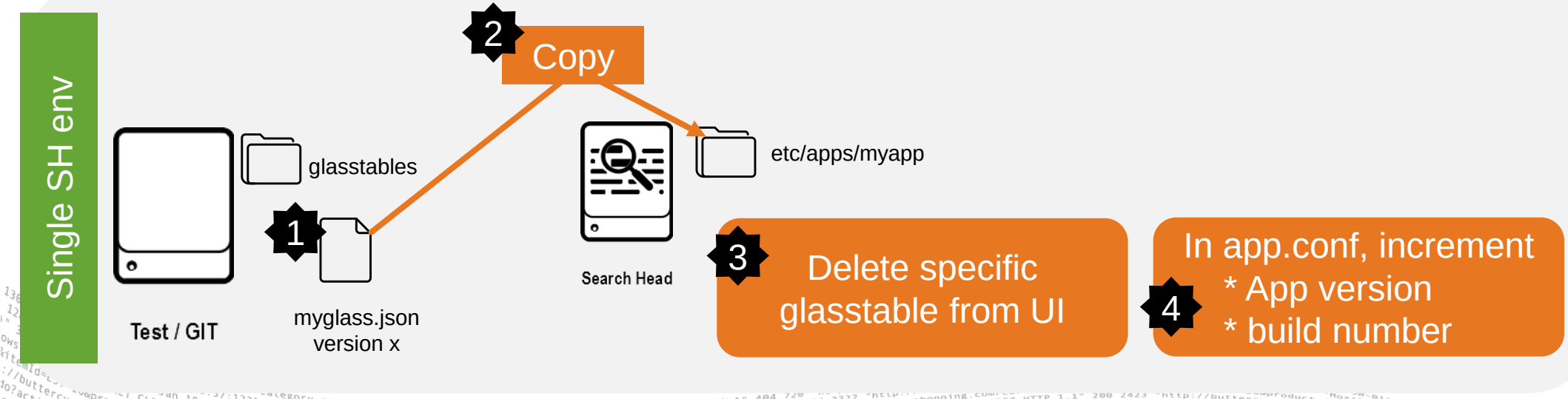
7 = | loadjob my_user:my_app:my_sched_search



Glass tables

Restore/deploy solution





splunk> .conf18

Glass tables

Happy Glasstables

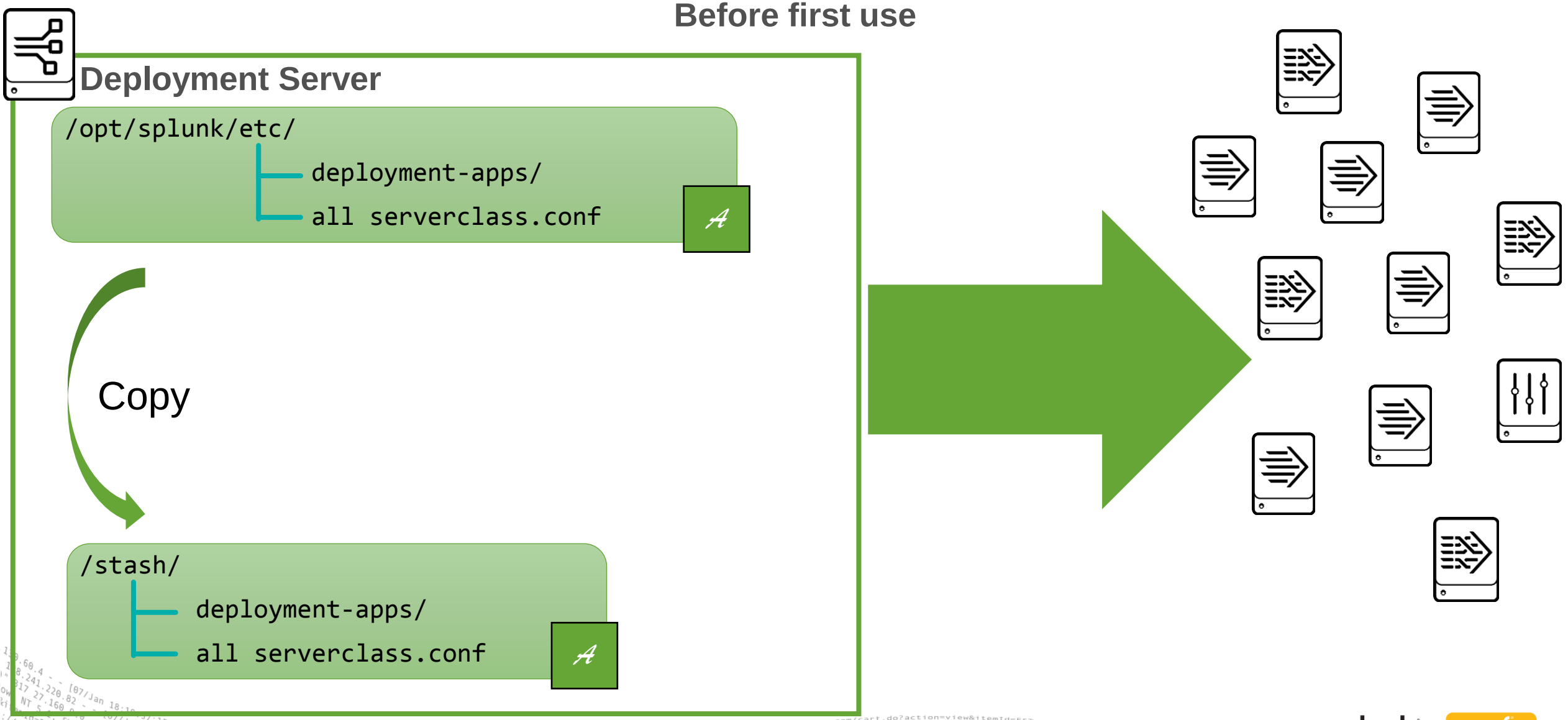
Just time for a quick recap

- 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

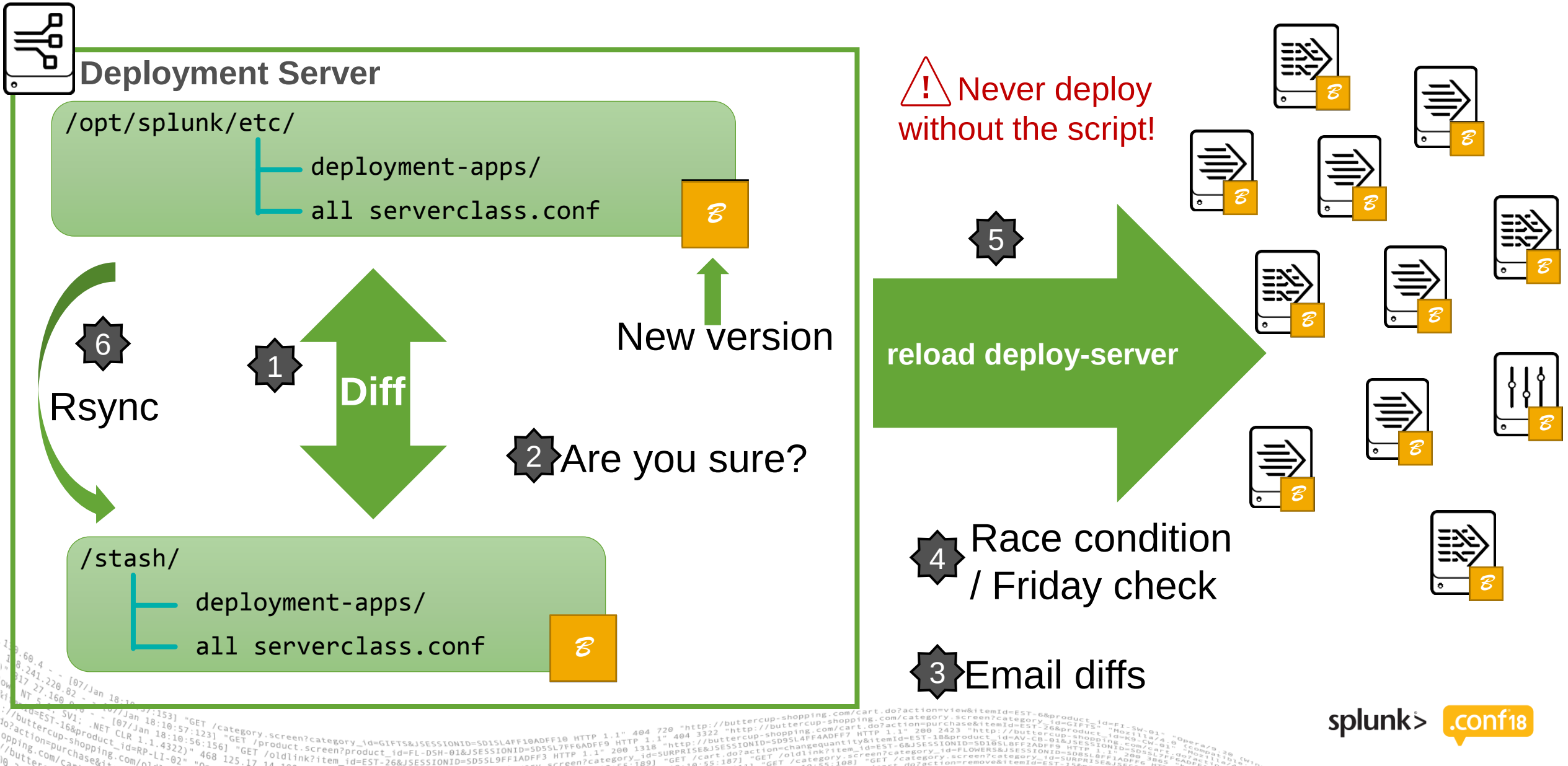
Deployment Server

reload deploy-server wrapper v1

Before first use



reload deploy-server wrapper v1



`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

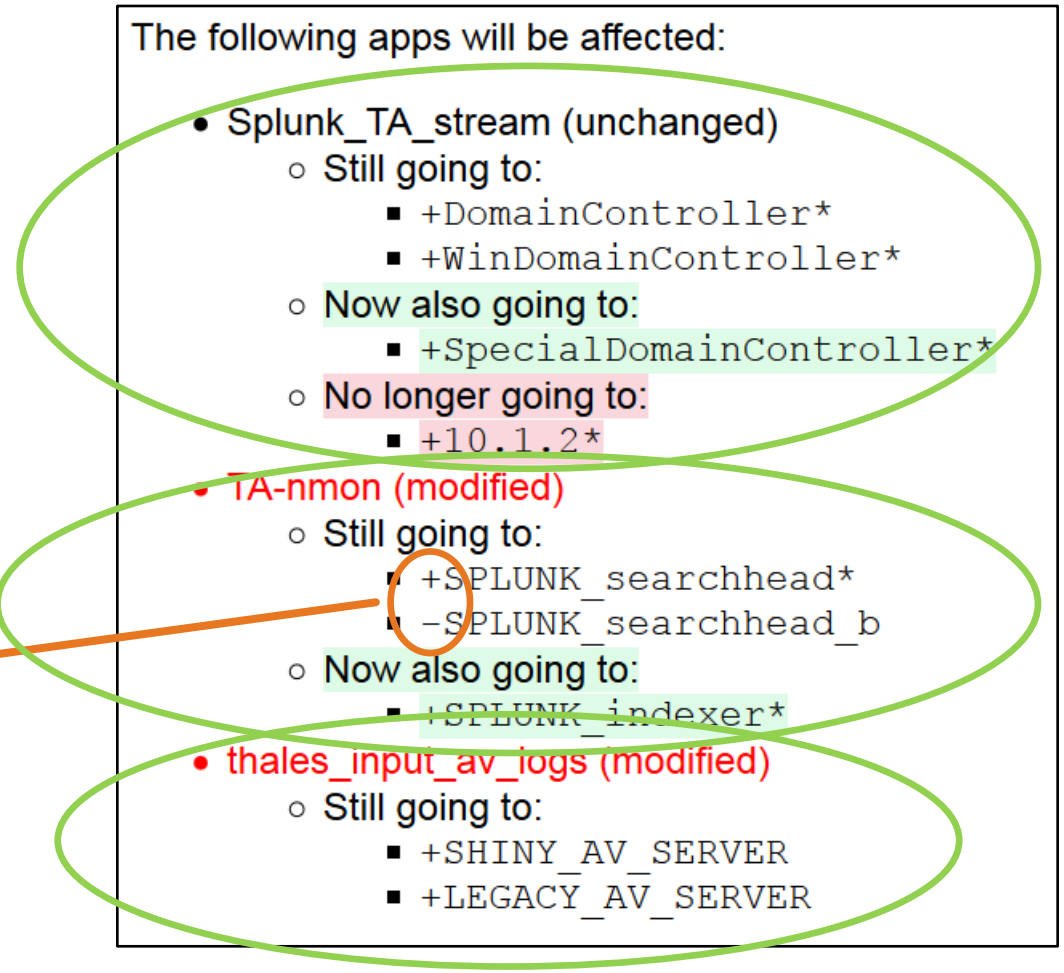
Summary = Most important improvement!

- 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]
```

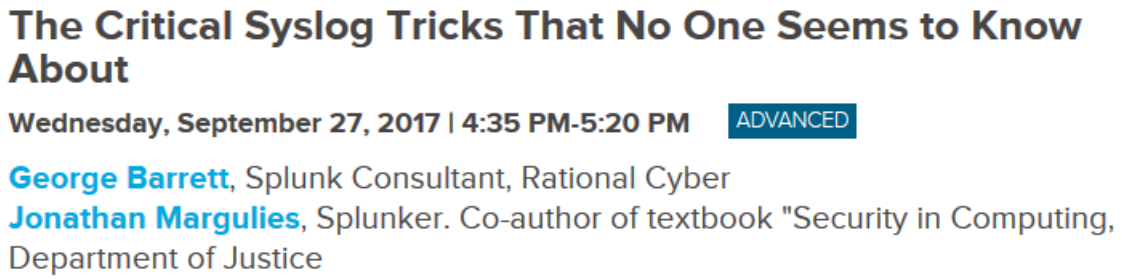


splunk> .conf18

`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

- ...

splunk> .conf18

`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/`

splunk> .conf18

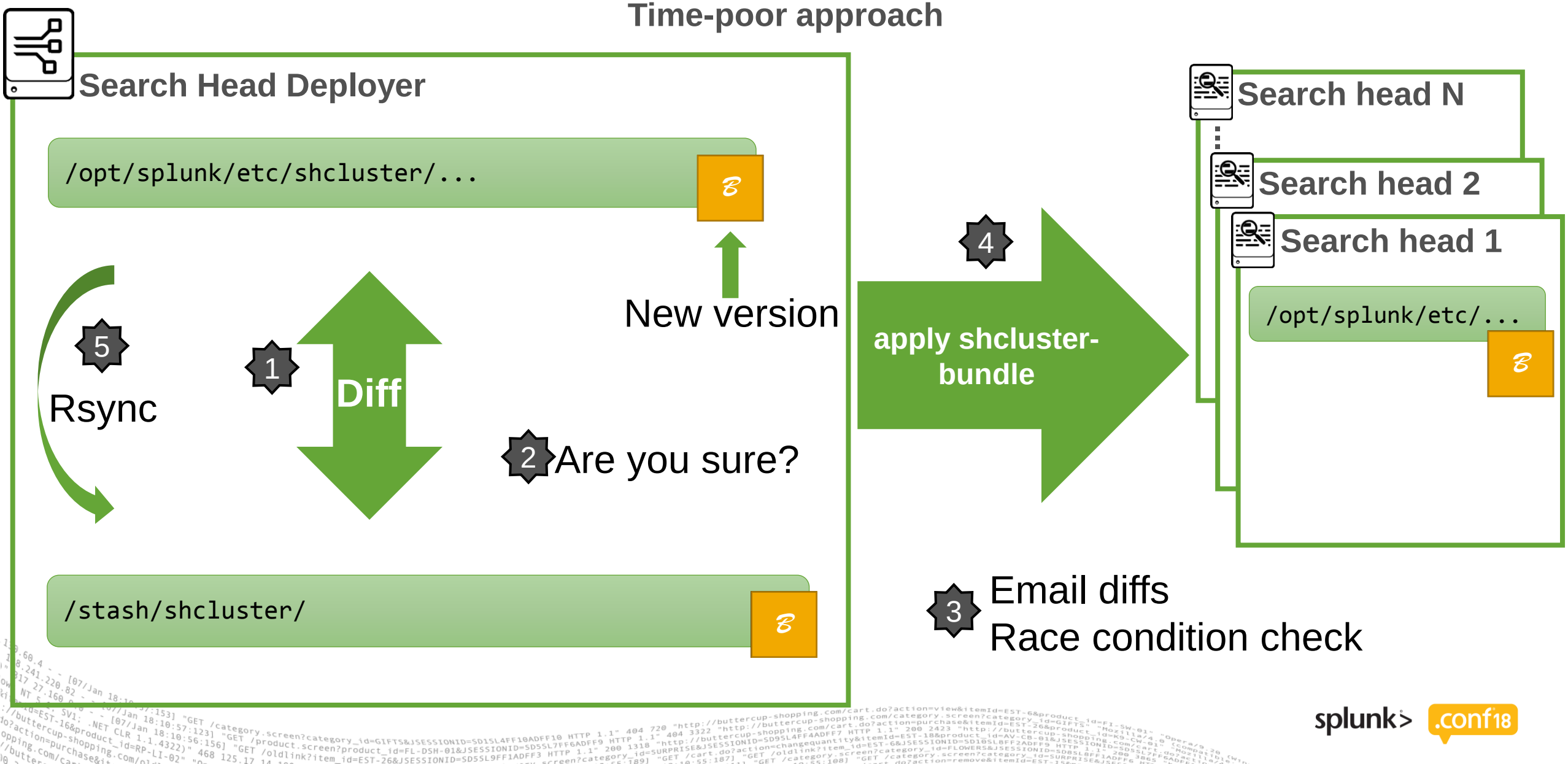
Just time for a quick recap

- 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



splunk> .conf18

`apply shcluster-bundle` wrapper v1

Advantages

- Easy

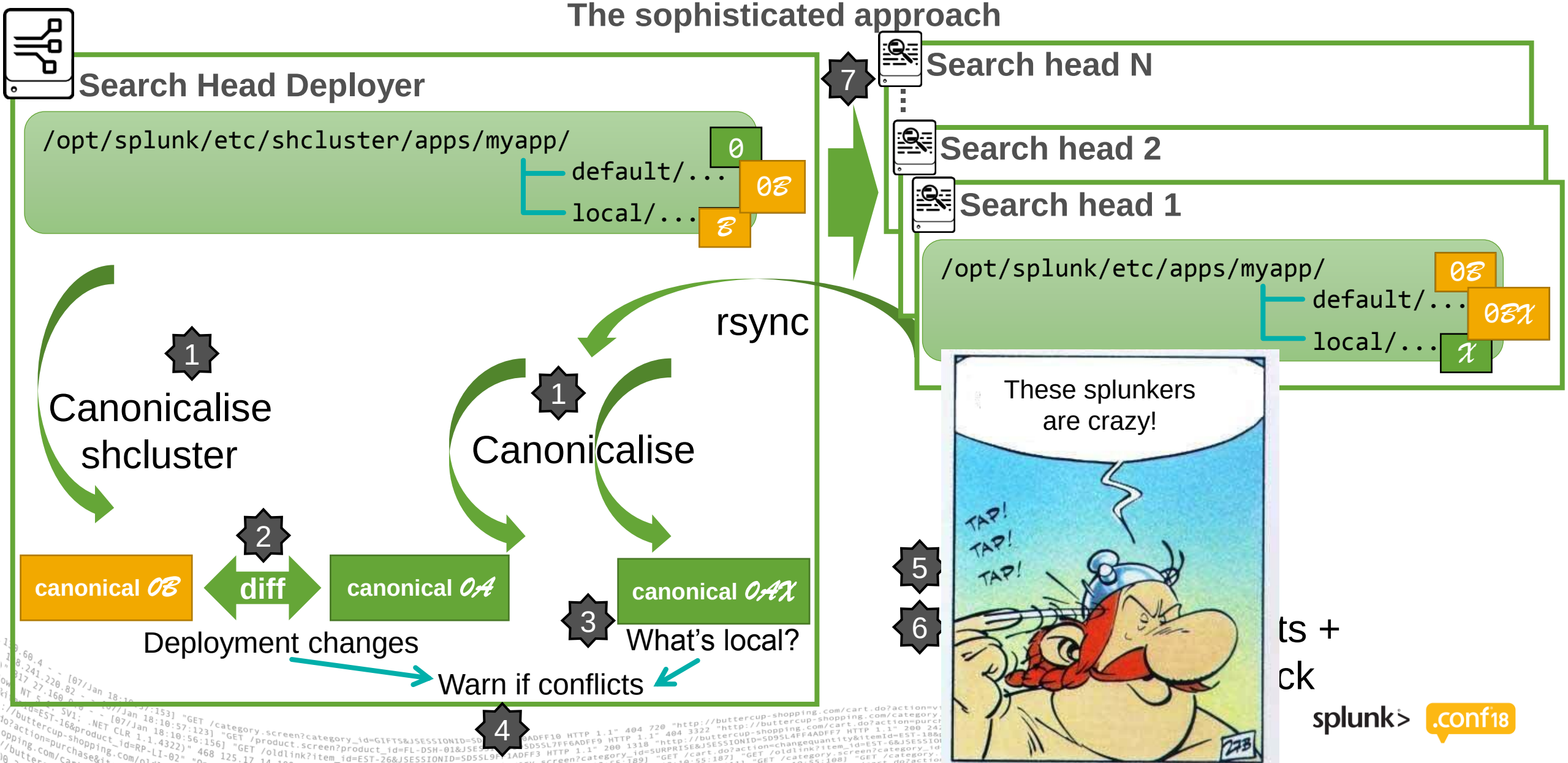
Disadvantages

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

splunk> .conf18

apply shcluster-bundle wrapper v2

The sophisticated approach



splunk> .conf18

`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

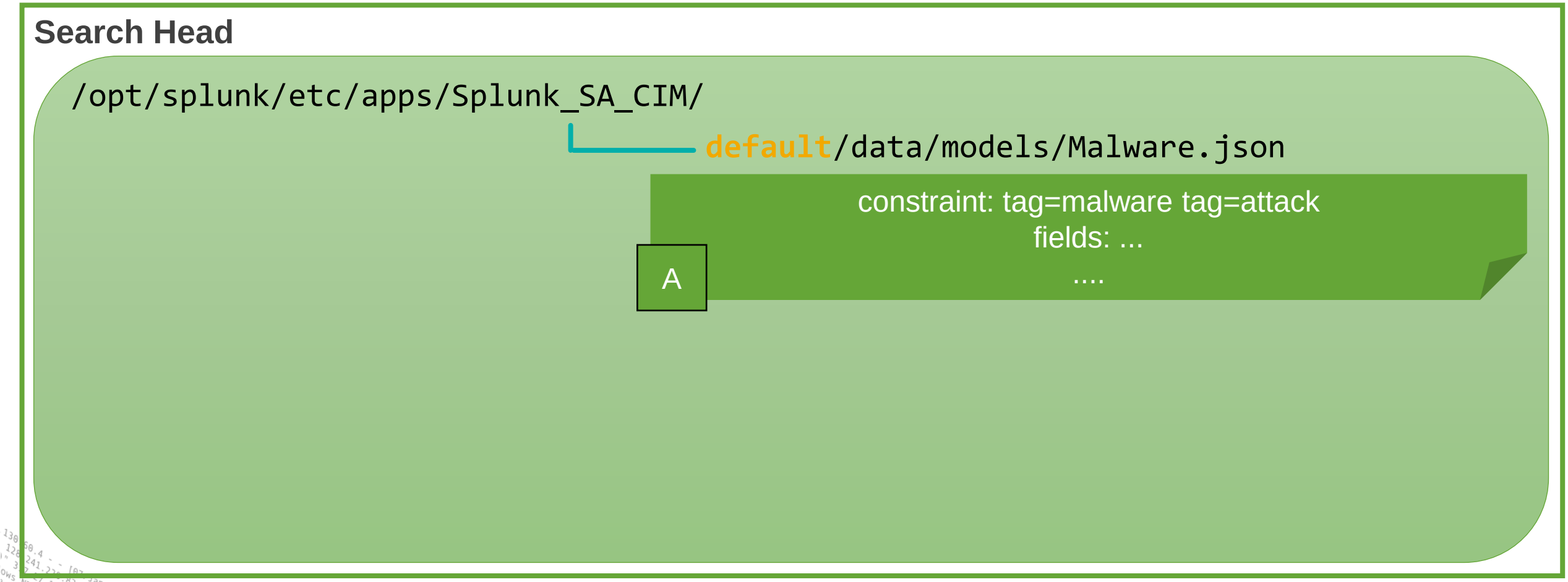
Just time for a quick recap

- 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

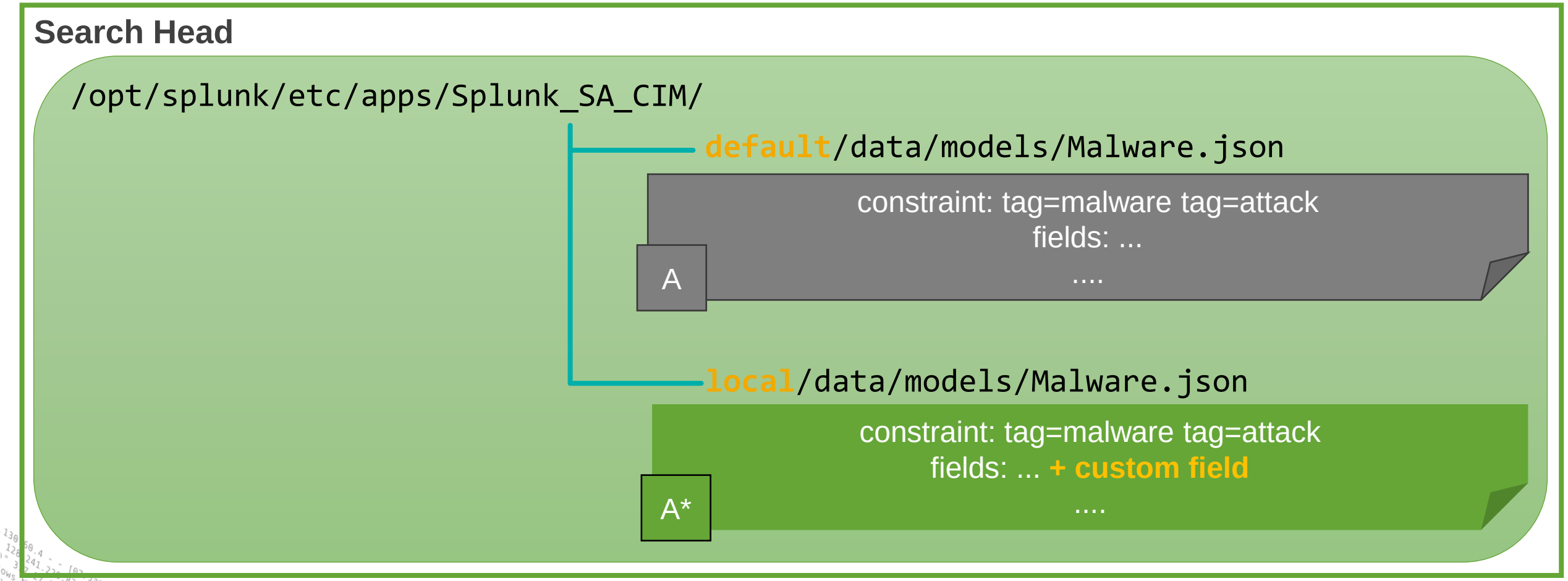
Precedence + upgrades = recipe for disaster

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



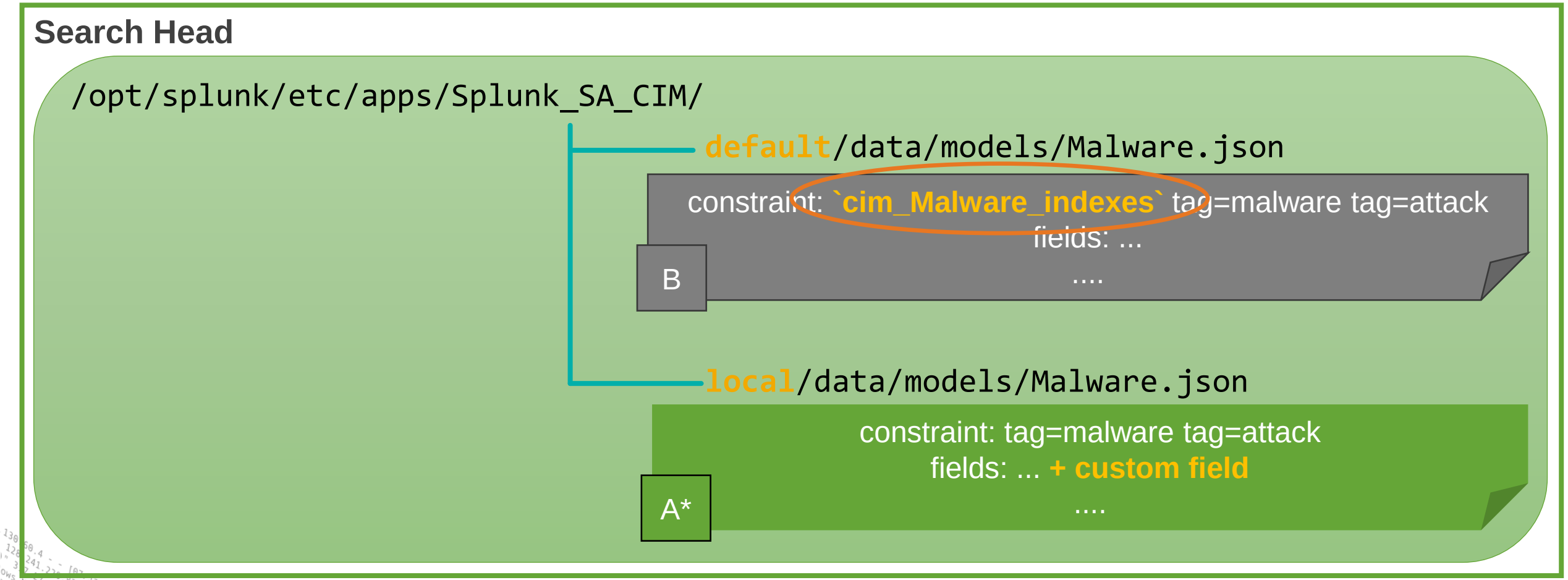
Precedence + upgrades = recipe for disaster

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



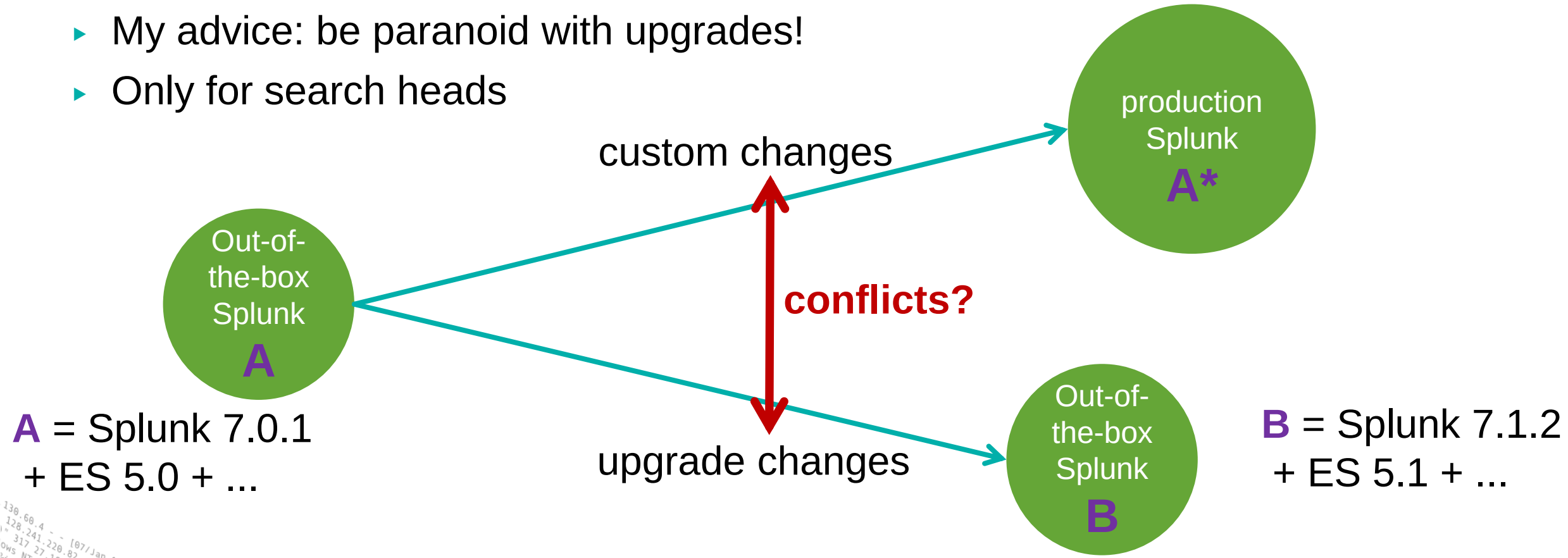
Precedence + upgrades = recipe for disaster

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

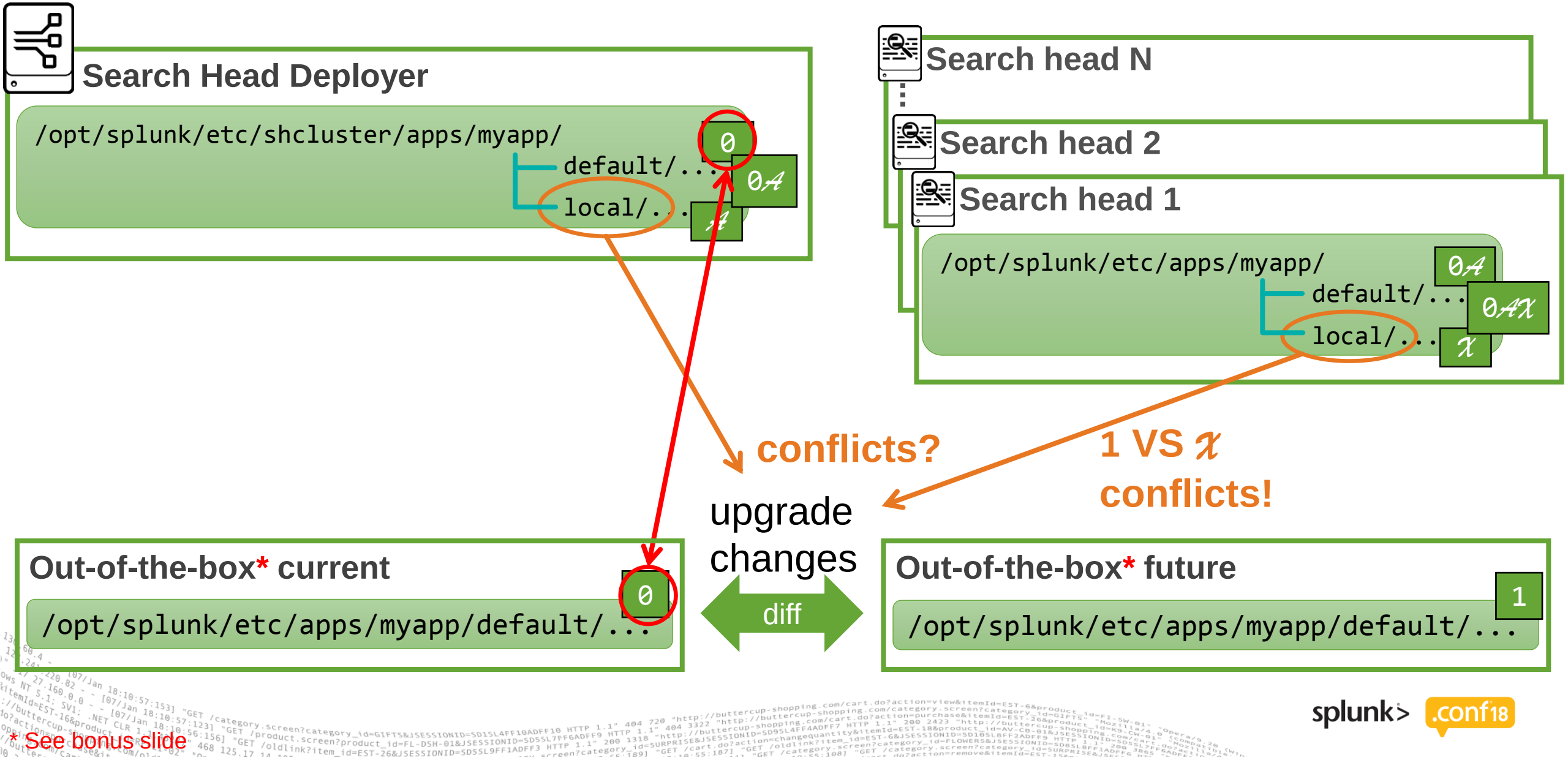


Upgrade strategy

- 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

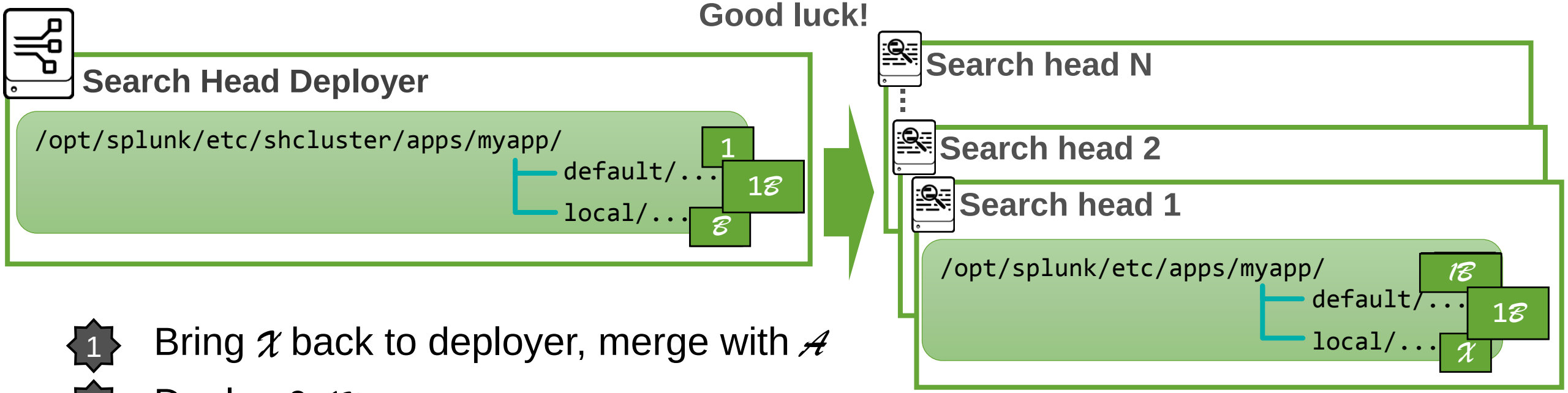


*See bonus slide

splunk> .conf18

Fixing upgrade conflict on a search head cluster

Good luck!



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

splunk> .conf18

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

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.”

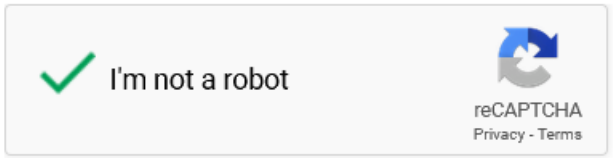
Last words

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



splunk> .conf18

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

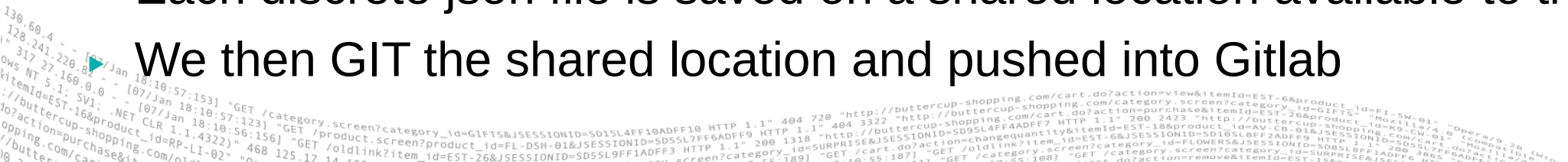
- “rsync --delete” to Mgmt/etc
- Delete all files in the Mgmt/etc_canonicalised folder (except the .git folder)
- Use canonicalise script to create Mgmt/etc_canonicalised from Mgmt/etc
- Then git both folders but don’t forget deleted files:

```
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



splunk> .conf18

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