



SplDevOps

Making Splunk Development a Breeze with a Deep Dive on DevOps, Containerization, Version Control & Automation

Harry McLaren, Ilias Diamantakos, Tomasz Dziwok

October 2018 | Version 1.3

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 Are We?



[cyberharibu](#)



HARRY MCLAREN

Splunk Enablement Lead, Managing Consultant

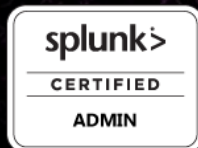


[ilias-diamantakos](#)



ILIAS DIAMANTAKOS

Splunk Engineer, Associate Consultant



Employer: ECS (UK Splunk Elite Partner)



Largest EMEA Splunk Delivery Partner
(Most Staff in Sales & Technical Areas)

Splunk's UK Based SME for Security

Managed SOC Provider

**Advanced Monitoring/Detection
Threat Hunting Services**



splunk>partner+

ELITE

AUTHORIZED RESELLER

splunk>

**REVOLUTION
AWARDS**

**2016 WINNER
SPLUNK PARTNER**

What's It All About?

- ▶ Customer Challenges
- ▶ What Do We Want?
- ▶ Our Idea to Deploy Splunk
- ▶ Technical Deep Dive
- ▶ Project Roadmap
- ▶ Key Takeaways



~40mins



Customer Challenges

“The expansion of Splunk has increased operational complexity, as we manage it manually and can’t keep on top of project change requests.”

– **High-Street Retailer**

“We require a full route-to-live to maintain system integrity and can’t deploy changes fast enough in our current setup.”

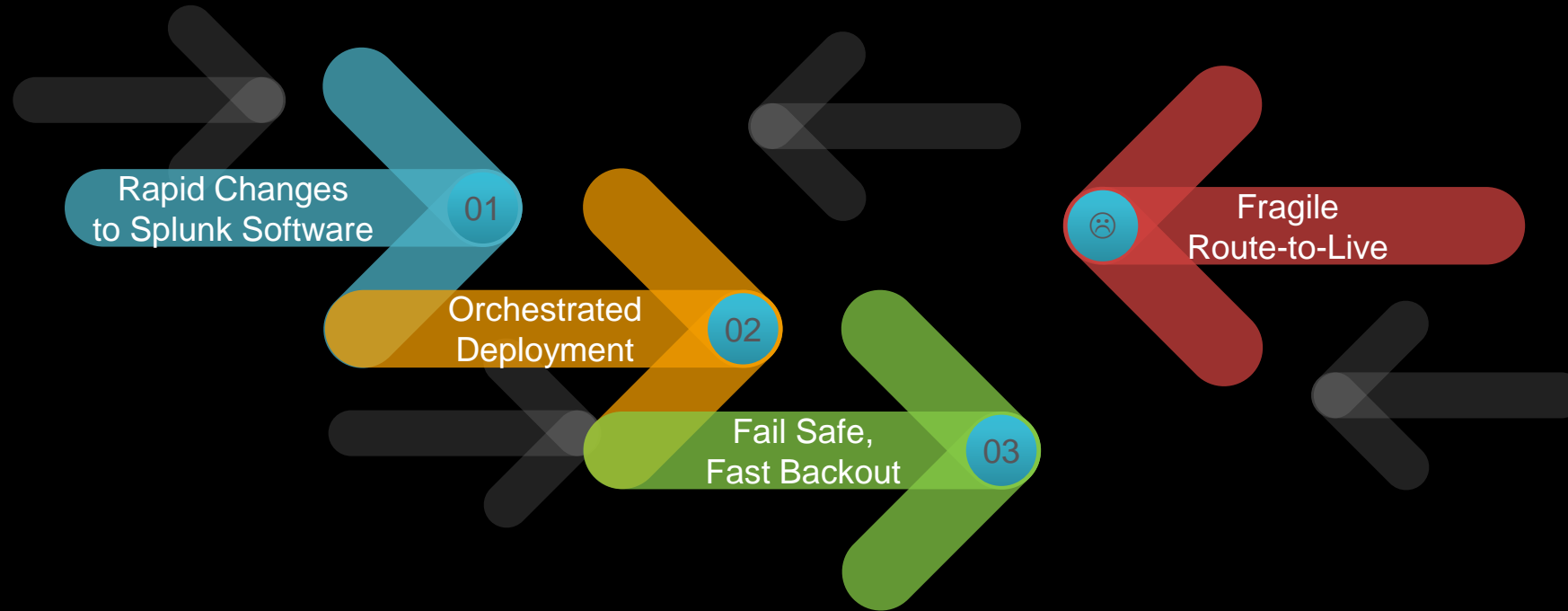
– **National Bank**

“Multiple developers within the same DEV environment, causes repeated configuration conflicts and delays to planned changes.”

– **National Building Society**

What Do We Want?

Enterprises Want to Respond Quickly, Safely & With Less Risk



Development at Scale

- ▶ Enterprise Scale Development
- ▶ Synchronous Changes / Multiple Admins & Developers
- ▶ Splunk Defined via Code
- ▶ Familiar Approach (AKA: DevOps/Agile)

Reduction in Custom Config

- ▶ Every 'Custom' Configuration Introduces Disparity
- ▶ Inconsistent Dev, Test, Pre-Prod, Prod
- ▶ Testing is "Best Endeavors"
- ▶ Increased Risk, Changes Batched



Splunk for Agility

Supporting Agile Methodology by Default



Monitor

SPL

Schema at Read,
Supporting Multiple Use Cases

Web UI

Analytic Tools Exposed to UI,
Empowering Users to Experiment

Plain Text Config

Plain Text Configuration Files,
Documented & Supported

Open API

Splunk API is Enumerated,
Dev Licenses, Labs Encouraged



Intelligence



Investigate

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0" "Opera/9.80"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0" "Chrome/60.0.3112.111"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0" "Chrome/60.0.3112.111"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0" "Opera/9.80"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0" "Chrome/60.0.3112.111"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0" "Chrome/60.0.3112.111"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0" "Opera/9.80"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0" "Chrome/60.0.3112.111"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3" "Mozilla/5.0" "Chrome/60.0.3112.111"
```


Our Idea

“SplDevOps” Became the Solution



Agile Development

- ✓ Short Sprints
- ✓ Test Driven Development
- ✓ Issue Management & Feature Backlog



Version Control

- ✓ Git[Lab] Utilized
- ✓ Multiple Projects/Branches
- ✓ Key Releases Tagged



Configuration Management

- ✓ Orchestrated Deployment
- ✓ Centralized Config
- ✓ Ansible used via SSH



Full Route-to-Live

- ✓ Multi-Stage Environments
- ✓ Dev > Pre-Prod > Prod
- Automated Testing





Project: Internal Monitoring

Ask: Deploy Splunk Internally for SecOps & ITOps Use Cases

Let's talk tools!



What Tool Fits Where?

a new Splunk infrastructure the DevOps way!

- ▶ Identical environments & route to live
 - Development, Pre-production, Production← Ansible + Git + Docker + Python
- ▶ Eliminate fear driven development
 - It's ok to make mistakes!← Docker + Git
- ▶ Minimize direct production changes
 - Always go through route-to-live
 - Transparent change control← GitLab
- ▶ Modern means of disaster recovery← Ansible (IaC)
- ▶ Security driven← Ansible Vault

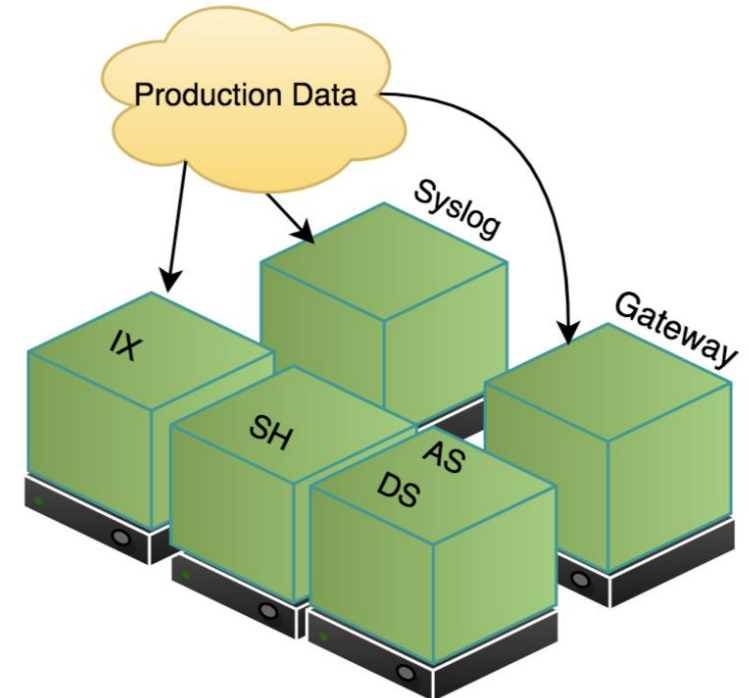
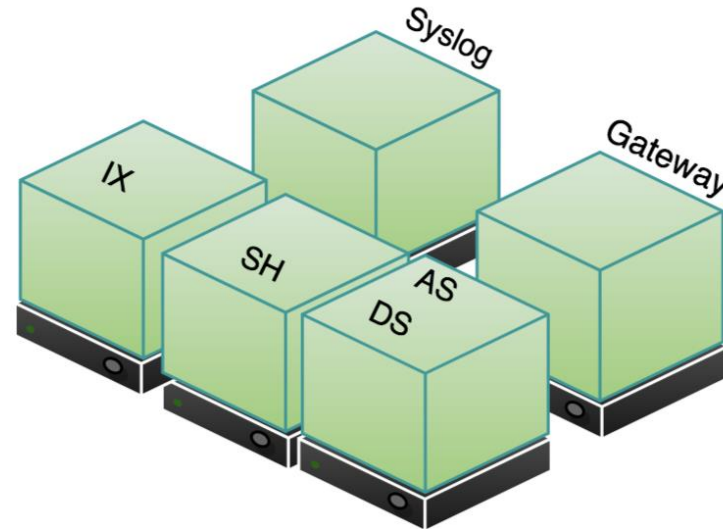
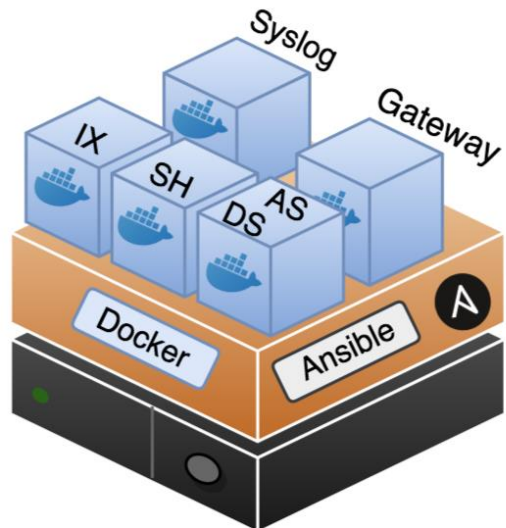
How We Wanted It To Look

Spoiler Alert: This is also the end result

dev

pre-prod

prod



IX: Splunk Indexer

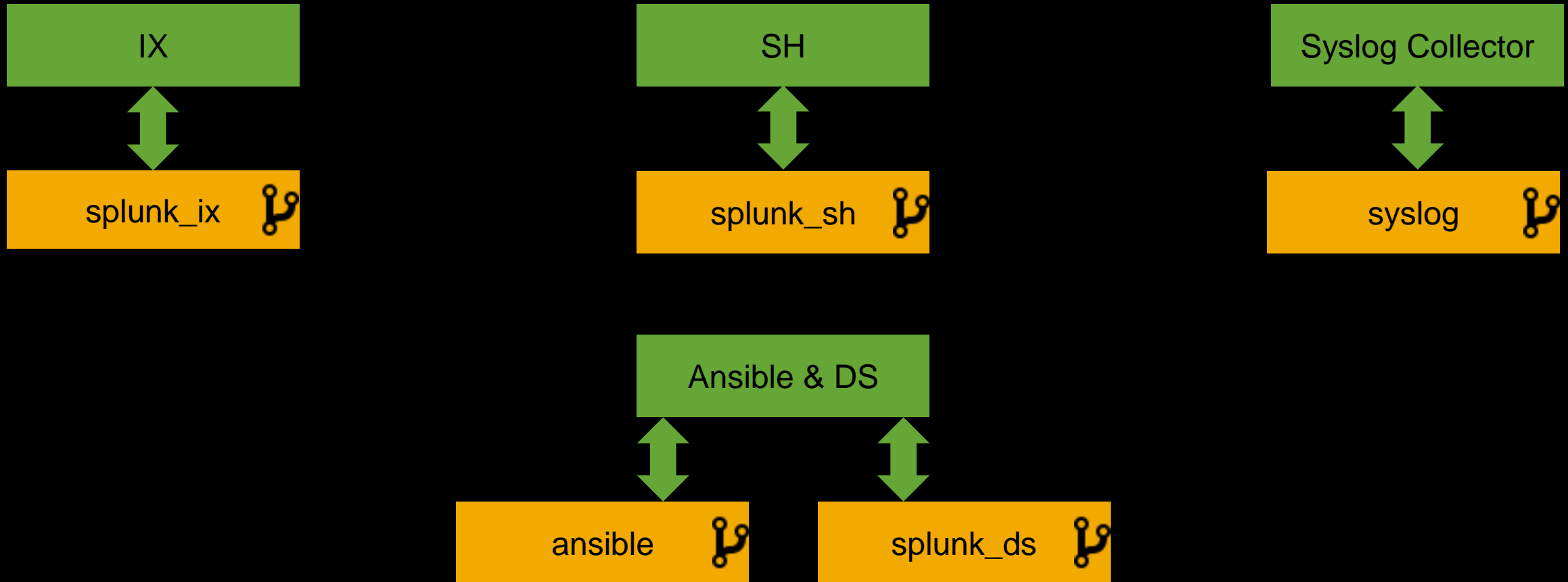
SH: Splunk Search Head

DS: Splunk Deployment Server

AS: Ansible Server

Multiple Repositories

Of /opt/splunk/etc for each instance



Git Workflow

aka “the change process”



Merge

Peer Review

dev

Merge

Senior Developer

pre-prod

Merge

Stakeholder

master

Release

Development Environment

Development Environment

Pre-production

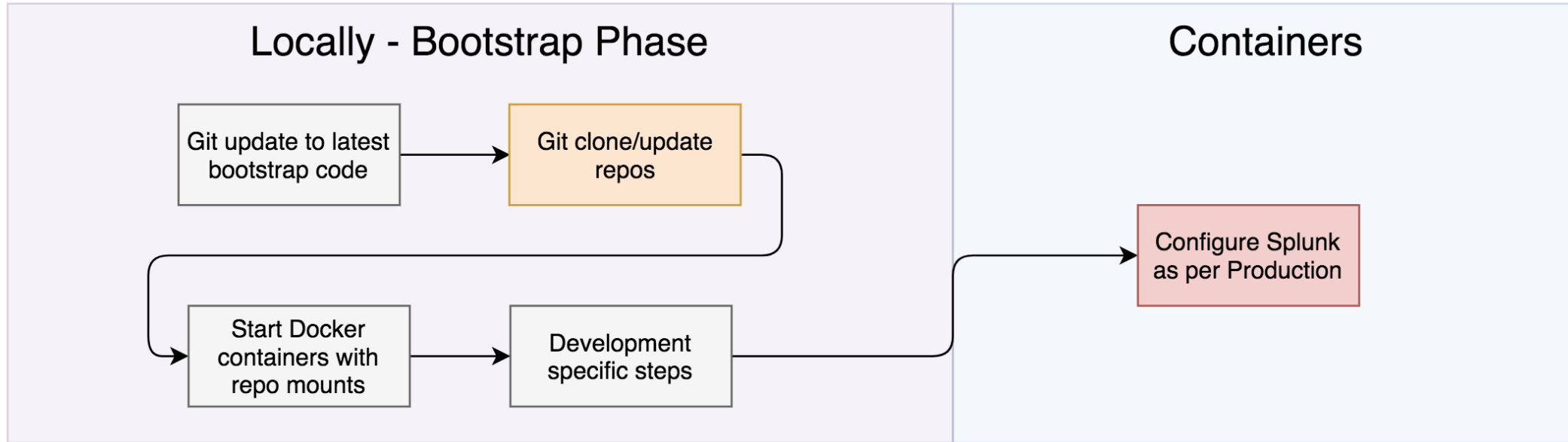
Production

Everything starts from our DevEnv

So let's spin one up

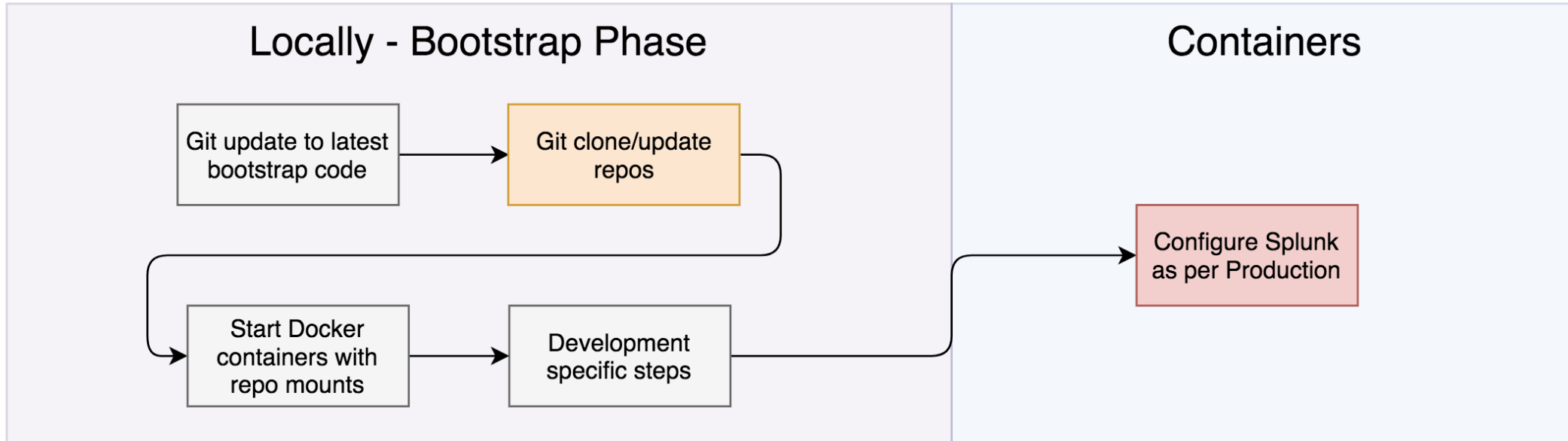
What's going on in the background

Development

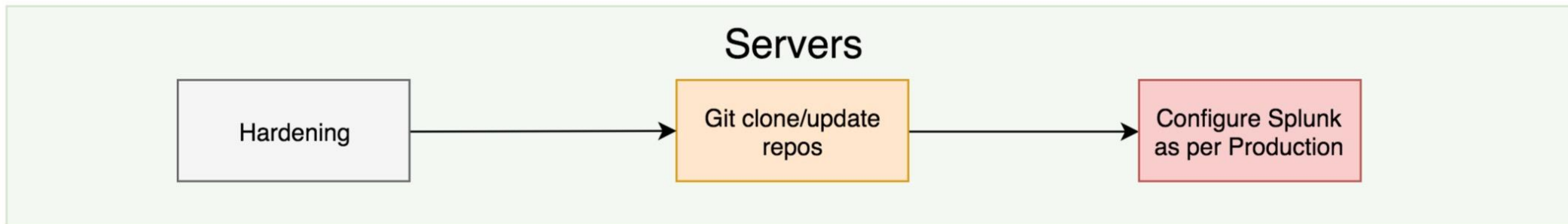


What's going on in the background

Development



Pre-Production /
Production



How It Looks

```
49 - name: Ensures auth dir exists
50   file:
51     path: "/opt/splunk/etc/auth"
52     state: directory
53     owner: splunk
54     group: splunk
55     become: True
56     become_user: root
57
58 - name: Write splunk.secret to IX and SH
59   copy:
60     dest: "/opt/splunk/etc/auth/splunk.secret"
61     content: "{{splunk_secret}}"
62     mode: 0400
63     owner: splunk
64     group: splunk
65
66
67 - name: Write admin passwd to IX and SH
68   lineinfile:
69     create: yes
70     path: "/opt/splunk/etc/passwd"
71     regexp: "^:admin:"
72     line: "{{admin_passwd}}"
73     mode: 0400
74     owner: splunk
75     group: splunk
76
```

How It Looks

```
49 - name: Ensures auth dir exists
50   file:
51     path: "/opt/splunk/etc/auth"
52     state: directory
53     owner: splunk
54     group: splunk
55   become: True
56   become_user: root
57
58 - name: Write splunk.secret to IX and SH
59   copy:
60     dest: "/opt/splunk/etc/auth/splunk.secret"
61     content: "{{splunk_secret}}"
62     mode: 0400
63     owner: splunk
64     group: splunk
65
66
67 - name: Write admin passwd to IX and SH
68   lineinfile:
69     create: yes
70     path: "/opt/splunk/etc/passwd"
71     regexp: "^:admin:"
72     line: "{{admin_passwd}}"
73     mode: 0400
74     owner: splunk
75     group: splunk
76
```


Let's Share Secrets

No really, we are sharing!

- ▶ How to version sensitive information
 - Encryption
- ▶ How to decrypt automatically
 - Ansible Vault
- ▶ How to store Ansible Vault Password
 - More encryption

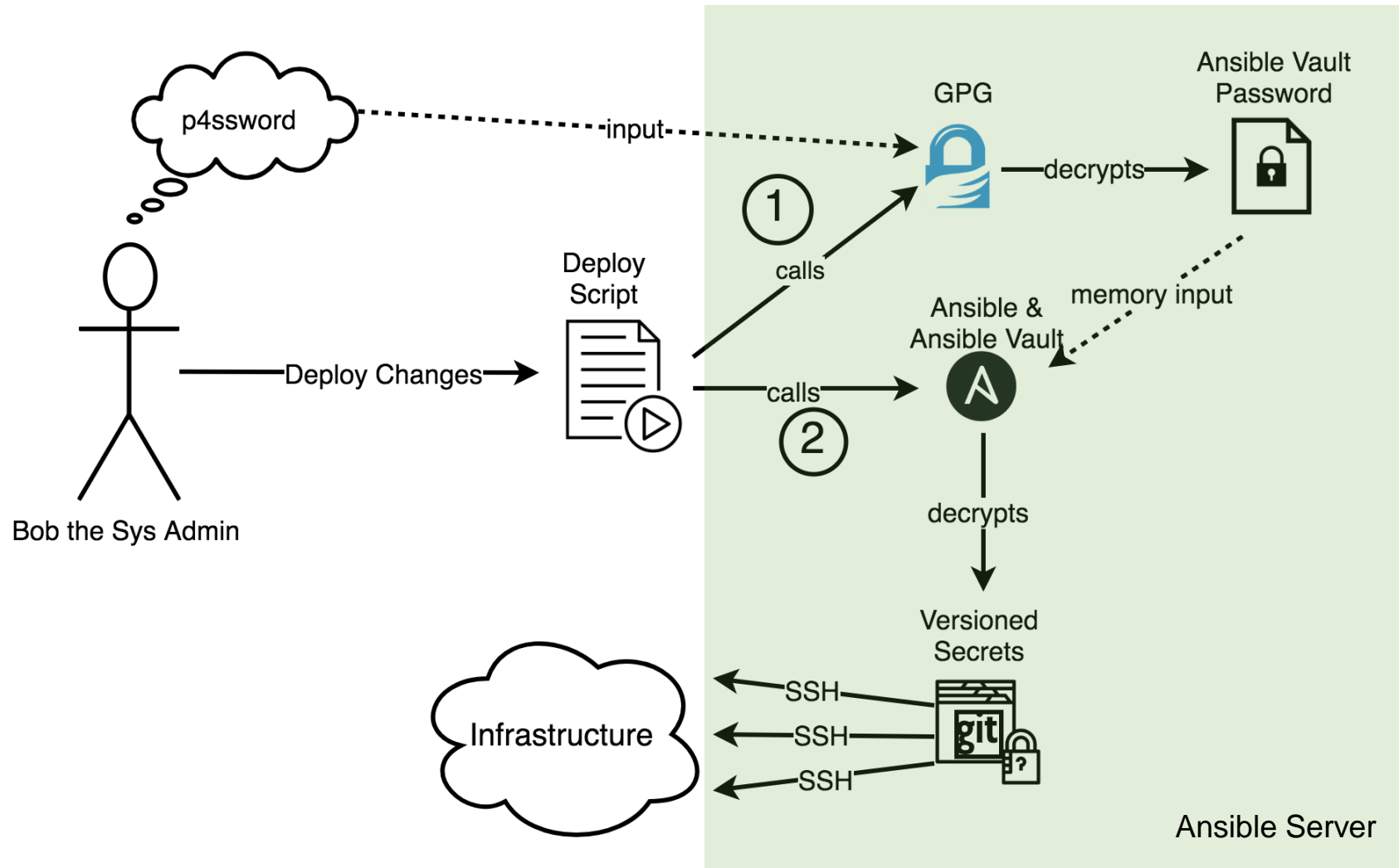
```

105 password: !vault |
106 $ANSIBLE_VAULT;1.1;AES256
107 32373930336665346139616562646432383365336462383039343439313335333835323330613363
108 3235663137326531333839353436413363306334326666370a616163633563626237623339633836
109 63656630393032353664343263613437386264303364346635633233653237383032396334396636
110 3932383836353265630a636564636362373831343534313536646333663337623561643861386465
111 38373532323066366430643738353265343737393564666538366332393065326433376463376565
112 38353066663535366135646665333662363534386434316236646337306637376237313963666433
113 35373239363930663561383932396535613937383265656239623435656531376332316139356664
114 34643563346263343164303136326662643334386431613264663562333933386436643965363037
115 62396430636632326439363532613431636535623866323361383835663362666133636665303634
116 343730643533373634333664613164613865616134363537333966303463373135323761393666131
117 653063653631393366373034366461633732343632633433386131646636623862313937303766633
118 34363266376431373161636164323932666434656361646238623330303336346665643536303163
119 39373734396462396138343632623461373565346638313534656634316166363031626239616232
120 32343561643433626132353562643735616162363231613932353439393834393634313131646537
121 33613761303536323932303836663431306666613038323130666332386266383433366635363336
122 62343230373736313463613562356537333633303738363663383233333437336266333135393661
123 66666132353639643166303434383235653539353634623733623637623831643266313533636138
124 36303532633933363465613861633539386231346133656365643037613836306132393161313366
125 34366466633538633565626666383631373966376463653464396139633034656431646137323435
126 36316261373631616535663838643763313236393337386338303764636639666333383161643063
127 61313333353136333735323239383730306161346531353034366666613764313363303439383261
128 3837346365333626363303936626538336666333961326434646365623038396461326262346436
129 66303032633434373061323565313330663263323861303064653930353865376162363261383732
130 63663133363931376561326136366437383337373462386562333131386662626139633862326233
131 36333361373539306335623739393761396530373866396261623838616533653439363166636563
132 32363135393735623865336265633730363634653264303732373763666563393835333335316533
133 37636561326530396236356533663832336164303930303833373637616630366239323433363636
134 65376637353861393534386432663562363964323764636537353831626334303830646332393061
135 38323834666238656439396538666463666533633365383961336364346431353533656139616338
136 333361635326633834373539653065383937303335353763623531343635346563666431623338
137 313533303765623434383236643566239313334353437396237303436364237653032393966303266
138 61363435653131616531366562356436356333646330356431353261343936326465386539336364
139 3837383339333233383265383663663656362626134643438326461636665633262

```

Let's Decrypt

One password to rule them all

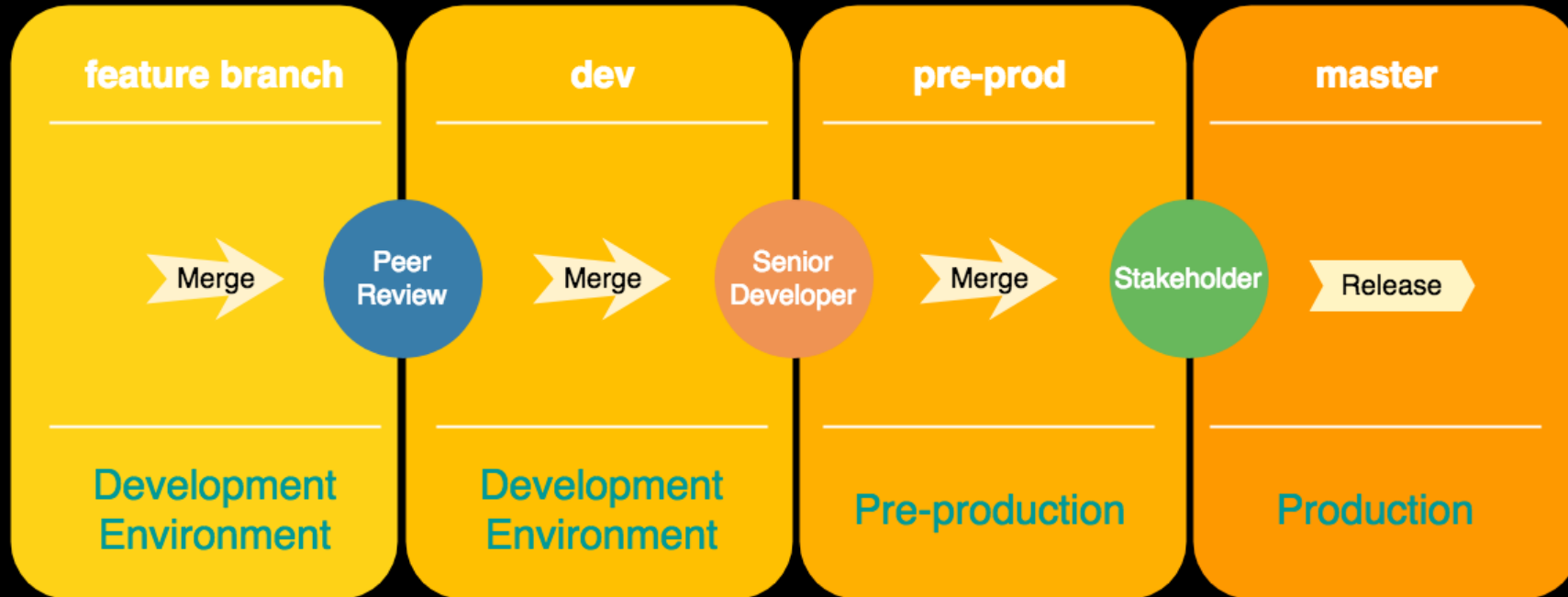


Use Case Scenario

Demo time

How it should have been done


Integrating with our change process



How it should have been done

Integrating with our change process

Open


Opened 1 minute ago by  **Tomasz Dziwok**


Edit

Close merge request

CHG-9876 : Update Dashboard


Fix issue with dashboard




Request to merge `conf-pres/dev`  **into** `dev`


Open in Web IDE

Check out branch


 ▼




Merge request approved

Approved by 

Ilias Diamantakos



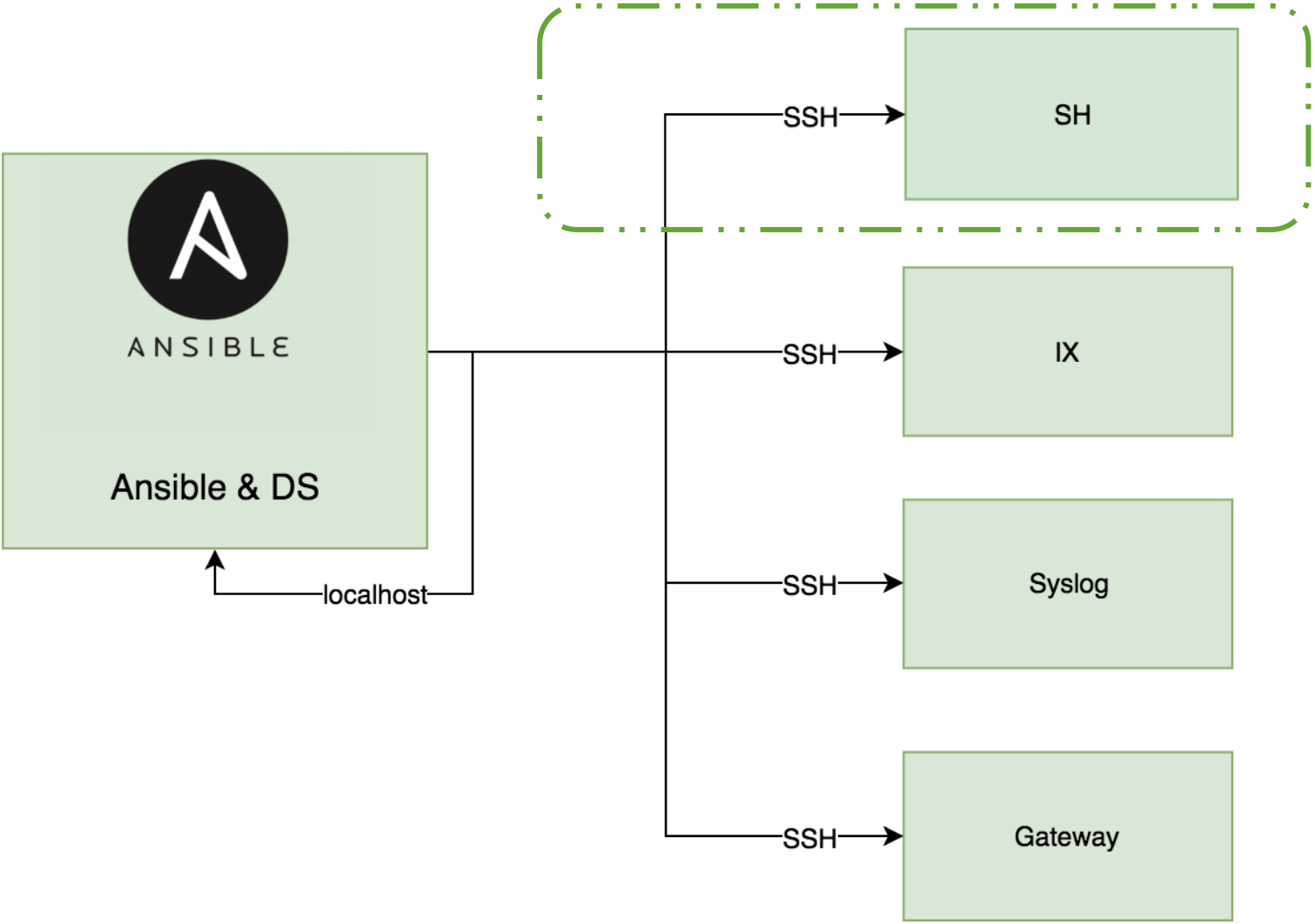
Merge

☐ Remove source branch ☐ Squash commits 

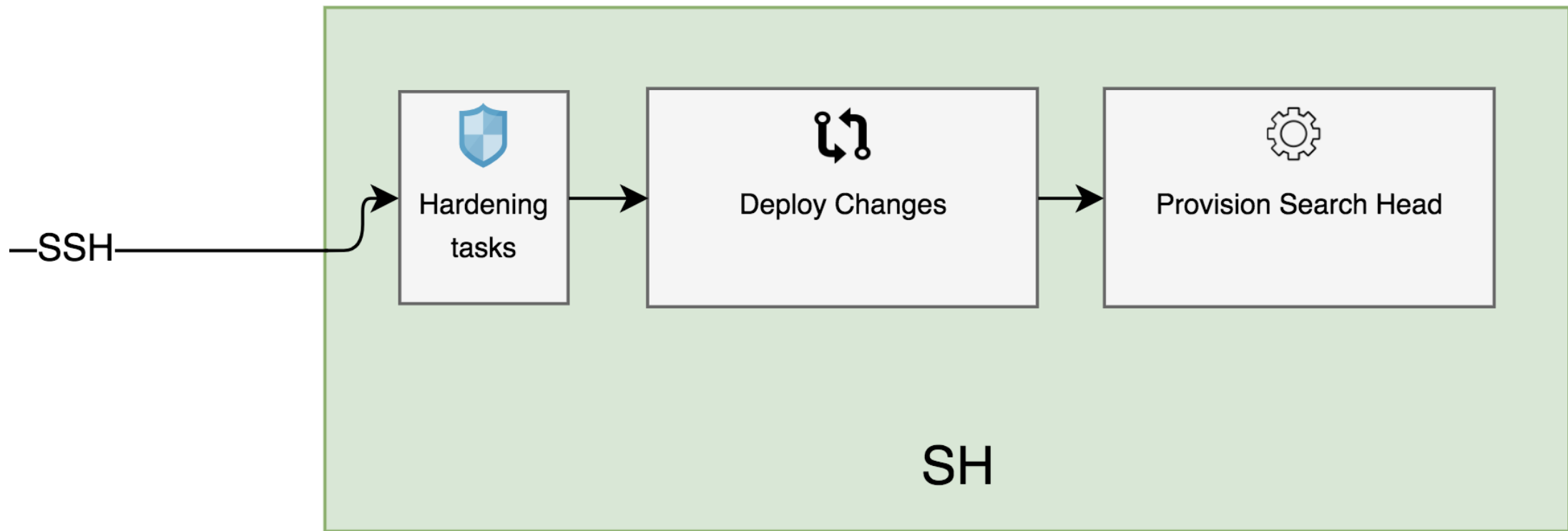
Modify commit message

You can merge this merge request manually using the [command line](#)

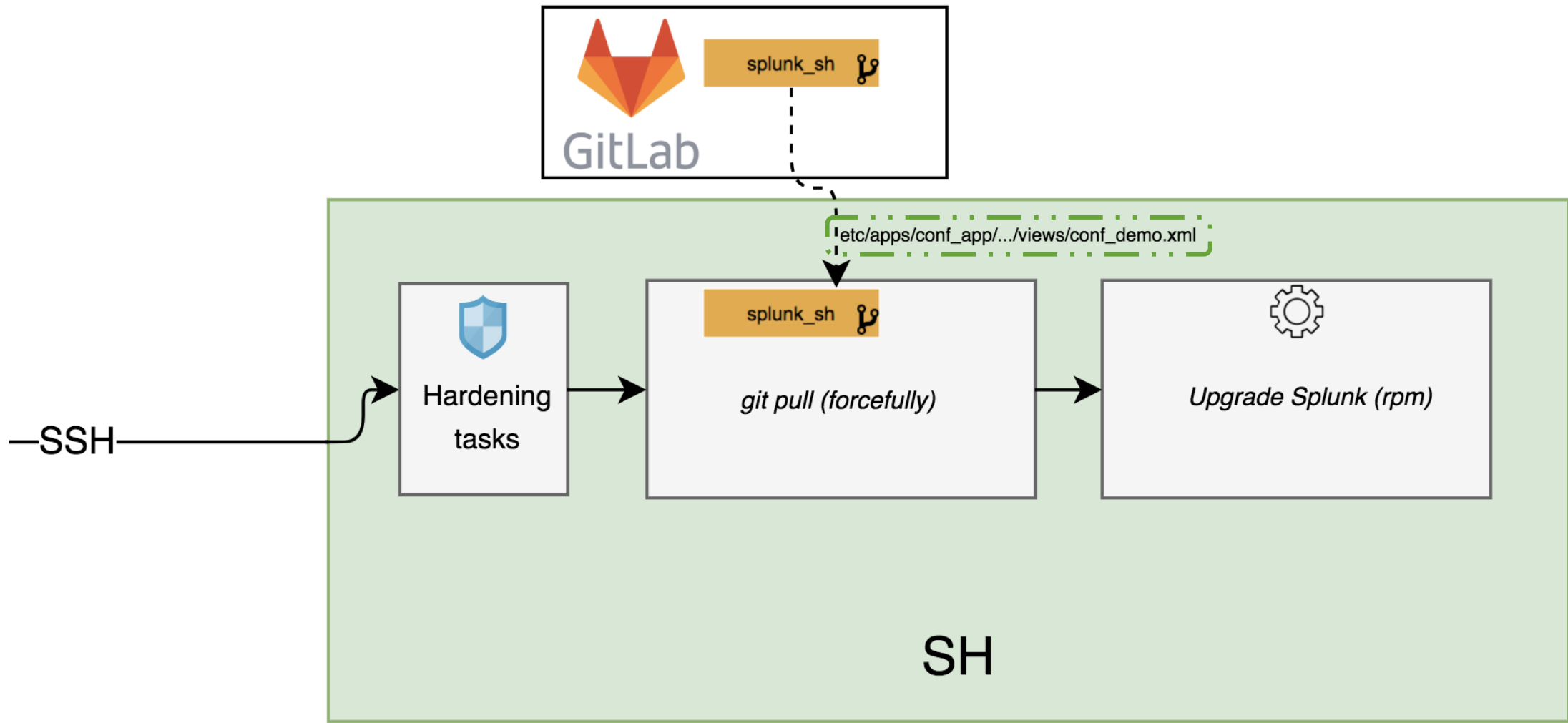
How it gets deployed



How it gets deployed



How it gets deployed



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/4.0 (compatible; Win...)"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/4.0 (compatible; Win...)"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-1B&product_id=AV-CB-01&SESSIONID=SD1B5LBFF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1K&product_id=SD5SL8FF1ADFF6 HTTP 1.1" 200 3865 "Mozilla/4.0 (compatible; Win...)"
100 125.17 14.11.11 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&SESSIONID=SD5SL8FF1ADFF6 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FI-SW-01" "Mozilla/4.0 (compatible; Win...)"

Lessons We Learned

Not everything was easy...

- ▶ Multiple repositories
 - What goes where?
 - Many lines of history
- ▶ Identical code for different environments
 - There are always exceptions (Eventgen, production API calls)
- ▶ Data for different environments
 - Production data is sensitive
- ▶ Automated deployment of code
 - When do you restart?



Deployment Results

Did it work!?

Prototype Success, Production Rollout



Introducing “Splunk Compiler” (v2.0+)



User Friendly &
End-to-End Integrated
with Issue/Change
Management

Key Takeaways

Remember Four Things...



Splunk Supports Experimentation by Default



Agile/DevOps Methodologies are Compatible



Doesn't Require Automation Expertise



Version Control **BEFORE** Software Orchestration

Thank You

Don't forget to **rate this session**
in the **.conf18** mobile app

.conf18

splunk>