

GENESIS

(THE SECRET SAUCE)



JAMES HUNT

Chief Architect

Stark & Wayne

@iamjameshunt

<https://github.com/jhunt>

<https://starkandwayne.com>

WHAT IS IT?



JAMES HUNT

STARK & WAYNE

BOSH AT SCALE



JAMES HUNT

STARK & WAYNE

BOSH AT SCALE

SECRETS MANAGEMENT



JAMES HUNT

BOSH AT SCALE
SECRETS MANAGEMENT
PRE-PACKAGED **BEST PRACTICES**



JAMES HUNT

STARK & WAYNE

BOSH AT SCALE
SECRETS MANAGEMENT
PRE-PACKAGED **BEST PRACTICES**
AUTOMATION FOR FREE



JAMES HUNT

STARK & WAYNE

A detailed architectural wireframe of a city skyline, featuring various skyscrapers and building structures. The lines are thin and light gray, set against a dark blue background. The perspective is from a low angle, looking up at the buildings.

GENESIS

BOSH

AT SCALE

**ALL CLOUD FOUNDRIES
LOOK THE SAME**



JAMES HUNT

STARK & WAYNE

SANDBOX

vs. DEV

vs. QA

vs. PROD



JAMES HUNT

STARK & WAYNE

DIFFER IN:

SIZING

SCALING

NAMING

NUMBERING

SANDBOX

vs. **DEV**

vs. **QA**

vs. **PROD**



JAMES HUNT

THEY FORM A **RUNWAY**

SANDBOX → DEV → QA → PROD



sw.yml

sw-us-east1.yml

sw-us-east1-sandbox.yml

sw-us-east1-dev.yml

sw-us-east1-qa.yml

sw-us-east1-prod.yml



sw.yml ←

sw-us-east1.yml

sw-us-east1-sandbox.yml

sw-us-east1-dev.yml

sw-us-east1-qa.yml

sw-us-east1-prod.yml

Global things

- kit name / version
- stemcell os / version
- whatever tickles your fancy



sw.yml

sw-us-east1.yml ←

sw-us-east1-sandbox.yml

sw-us-east1-dev.yml

sw-us-east1-qa.yml

sw-us-east1-prod.yml

IaaS things

- cloud config names
- blobstore types (S3, GCS, etc.)
- database engines (i.e. RDS)
- whatever floats your boat



sw.yml

sw-us-east1.yml

sw-us-east1-sandbox.yml ←

sw-us-east1-dev.yml ←

sw-us-east1-qa.yml ←

sw-us-east1-prod.yml ←

Environment things

- names
- how many VMs?
- connection strings
- specific features (e.g. HA or not)
- whatever flips your pancake



**THIS STRUCTURE IS
IMPORTANT FOR CI/CD**

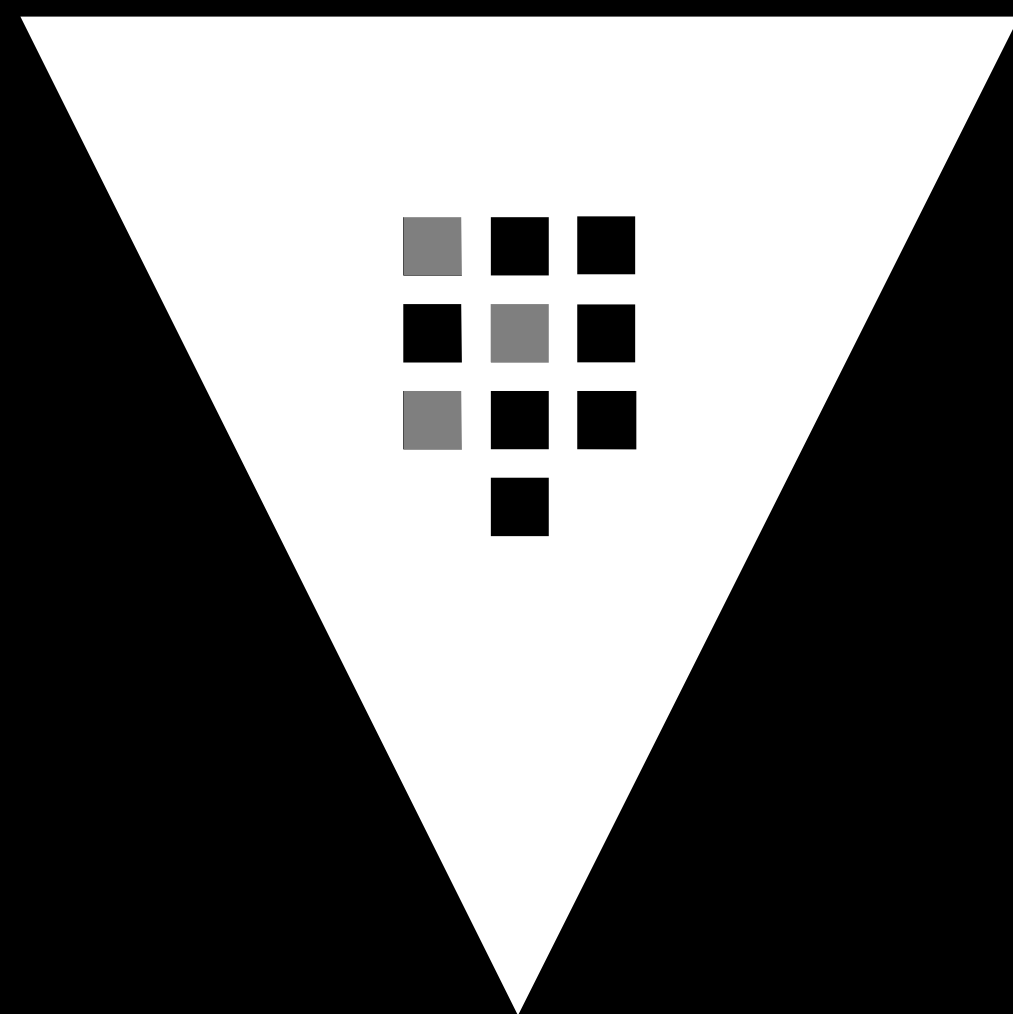


JAMES HUNT

A detailed architectural wireframe of a skyscraper, rendered in a light gray color against a dark blue background. The wireframe shows the intricate structural elements of the building, including the facade, internal framework, and various levels. The building is oriented vertically, with its base at the bottom and its top reaching towards the top of the frame. The lines are thin and precise, creating a complex geometric pattern.

GENESIS

**SECRETS
MANAGEMENT**



HashiCorp

Vault



JAMES HUNT

STARK & WAYNE

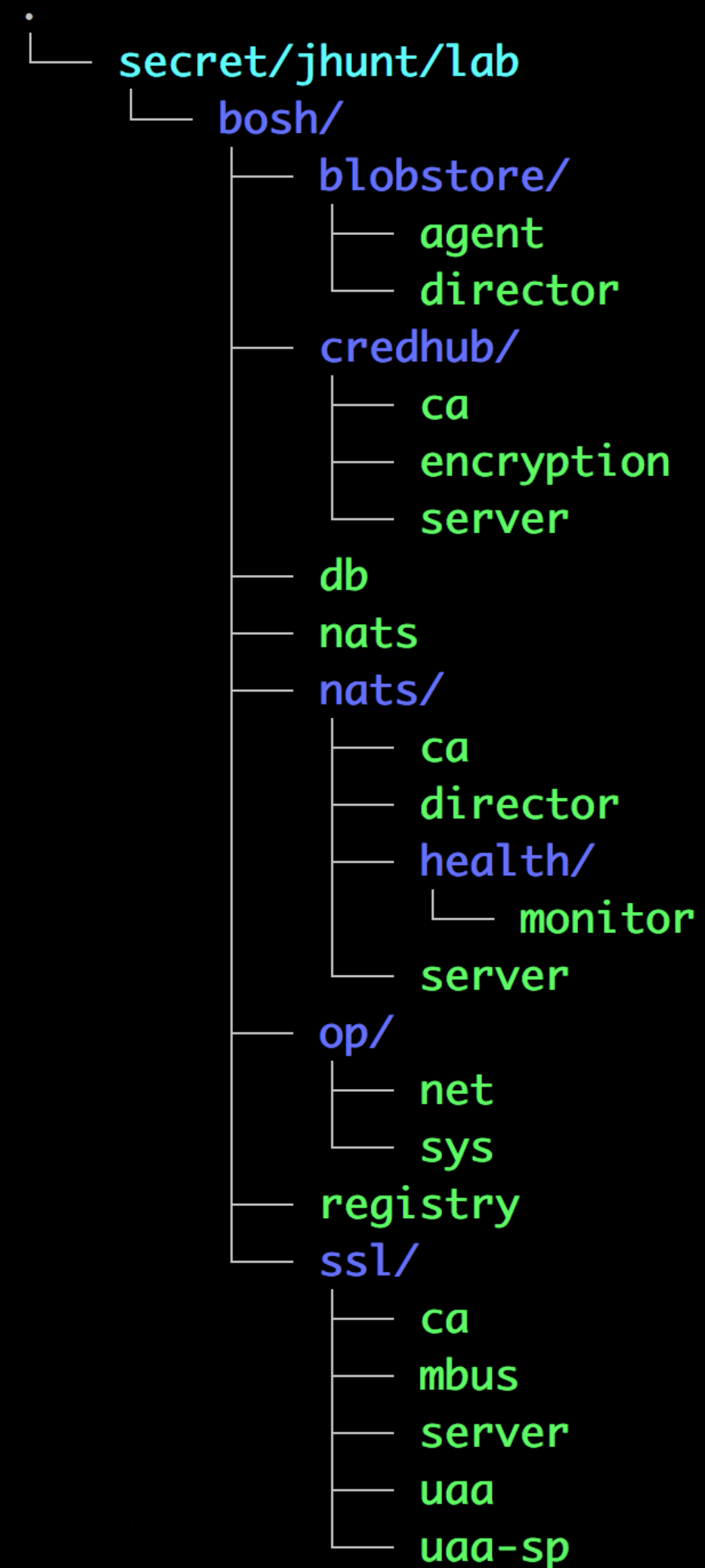
**EVERY GENESIS SITE
HAS ONE VAULT**



JAMES HUNT

STARK & WAYNE

→ safe tree secret/jhunt/lab



GENESIS MANAGES SECRETS FOR YOU

\$ genesis **new**

\$ genesis **add-secrets**

\$ genesis **rotate-secrets**



```
credentials:
  base:
    op/net: ssh 4096
    op/sys:
      password: random 12 fmt crypt-sha512

  blobstore/agent:
    password: random 64 fixed
  blobstore/director:
    password: random 64
  db:
    password: random 64
  nats:
    password: random 64 fixed
  registry:
    password: random 64 fixed
```

KITS DEFINE THE CREDENTIALS

passwords
SSH keys
RSA keys



KITS DEFINE THE CERTIFICATES

Certificate Authorities
Key Usage Constraints
Certificate Expiration
Subject Alternate Names

```
certificates:  
  base:  
    ssl:  
      ca: { valid_for: 1y }  
      server:  
        valid_for: 1y  
        names:  
        - ${params.static_ip}  
      mbus:  
        valid_for: 1y  
        names:  
        - ${params.static_ip}  
      uaa:  
        valid_for: 1y  
        names:  
        - ${params.static_ip}  
      uaa-sp:  
        valid_for: 1y  
        names:  
        - ${params.static_ip}
```



BOSH

3 CAS
8 CERTS

CLOUD FOUNDRY

12 CAS
58 CERTS

BLACKSMITH

2 CAS
4 CERTS

SHIELD

2 CAS
2 CERTS



JAMES HUNT

STARK & WAYNE

**ALL PROPERLY
GENERATED AND ROTATED
(FOR FREE)**



JAMES HUNT

**THIS TOO IS
IMPORTANT FOR CI/CD**



JAMES HUNT

A detailed architectural wireframe of a skyscraper, rendered in a light gray color against a dark blue background. The drawing shows the complex structural framework of the building, including its vertical columns, horizontal beams, and various levels of scaffolding or construction elements. The perspective is from a low angle, looking up at the tower, which emphasizes its height and scale. The lines are clean and precise, typical of architectural blueprints.

GENESIS

**BEST
PRACTICES**

KITS



JAMES HUNT

STARK & WAYNE

```
kit:
```

```
  name:    bosh
```

```
  version: 1.1.3
```

```
  features:
```

```
    - vsphere
```

```
params:
```

```
  env:    jhunt-lab
```

```
  static_ip: 10.200.192.0
```

```
  bosh:      buffalo-lab
```

Kit Name

- what are we deploying?




```
kit:
```

```
  name:    bosh
```

```
  version: 1.1.3
```

```
  features:
```

```
    - vsphere
```

Kit Version

```
params:
```

```
  env:    jhunt-lab
```

```
  static_ip: 10.200.192.0
```

```
  bosh:      buffalo-lab
```



kit:

name: bosh

version: 1.1.3

features:

- vsphere



Features

- enable an optional configuration
- choose one from many
- affect how Genesis behaves

params:

env: jhunt-lab

static_ip: 10.200.192.0

bosh: buffalo-lab



```
kit:  
  name:    bosh  
  version: 1.1.3  
  features:  
    - vsphere
```

```
params: ←  
  env:    jhunt-lab  
  
  static_ip: 10.200.192.0  
  bosh:      buffalo-lab
```

Parameters

- common configuration knobs
- levers you can pull
- often cascade through the manifest



```
kit:  
  name:    bosh  
  version: 1.1.3  
  features:  
    - vsphere  
  
params:  
  env:    jhunt-lab  
  
  static_ip: 10.200.192.0  
  bosh:      buffalo-lab  
  
instance_groups:  
  - name: bosh  
    vm_type: super-duper-extra-large  
    properties:  
      genesis: is awesome
```

**YOU STILL HAVE
ACCESS TO THE
BOSH MANIFEST**



**OPERATORS SHOULD HAVE
A SAY IN HOW THINGS
GET DEPLOYED**



JAMES HUNT

A detailed architectural wireframe of a modern skyscraper, rendered in a light gray color against a dark blue background. The structure features multiple levels, balconies, and a complex network of lines representing the building's framework. The perspective is from a low angle, looking up at the tower.

GENESIS

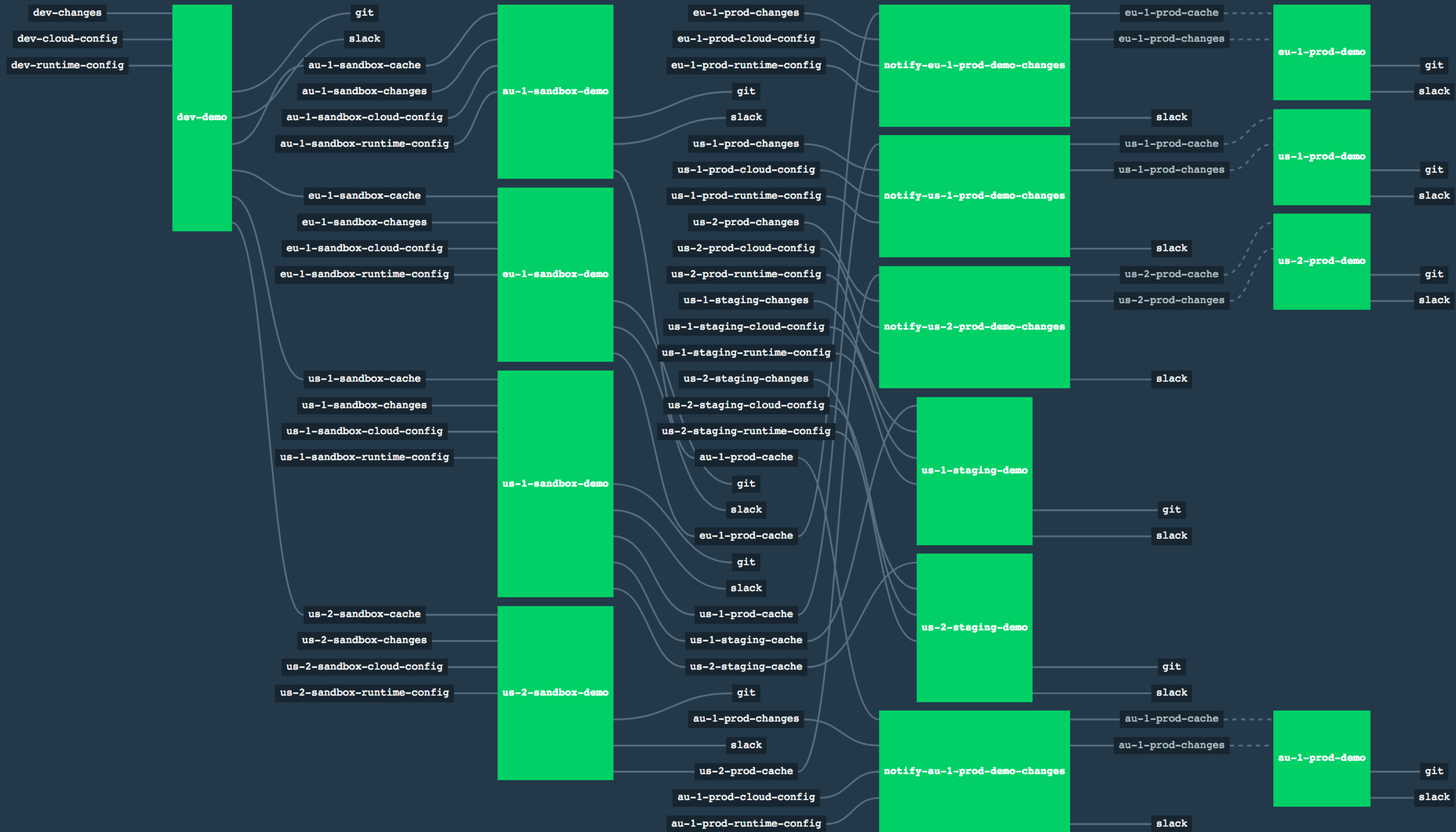
CI/CD

AUTOMATION

IF YOU AIN'T **AUTOMATIN'**
YOU AIN'T **OPERATIN'**



JAMES HUNT



JAMES HUNT

STARK & WAYNE



JAMES HUNT

STARK & WAYNE

```
groups:
- jobs
- au-1-prod-demo
- au-1-sandbox-demo
- dev-demo
- eu-1-prod-demo
- eu-1-sandbox-demo
- us-1-prod-demo
- us-1-sandbox-demo
- us-1-staging-demo
- us-2-prod-demo
- us-2-sandbox-demo
- us-2-staging-demo
- notify-au-1-prod-demo-changes
- notify-eu-1-prod-demo-changes
- notify-us-1-prod-demo-changes
- notify-us-2-prod-demo-changes
name: cfsummit2018
jobs:
- name: notify-au-1-prod-demo-changes
  plan:
  - aggregate:
    - get: au-1-prod-changes
      trigger: true
    - get: au-1-prod-cloud-config
      trigger: true
    - get: au-1-prod-runtime-config
      trigger: true
    - get: au-1-prod-cache
      passed:
        - au-1-sandbox-demo
      trigger: true
    - aggregate:
      - params:
          channel: slackjbaaskjhdfkj
          icon_url: http://ci.ly/image/3e1h0h3k2e0p/
        concourse-logo.png
      text: "cfsummit2018: Changes are staged to be
        deployed to au-1-prod-demo.
        please schedule a run a deploy via Concourse"
        username: runwaybot
      put: slack
      public: true
      serial: true
  - name: au-1-prod-demo
    plan:
    - do:
      - aggregate:
        - get: au-1-prod-changes
          passed:
            - notify-au-1-prod-demo-changes
          trigger: false
        - get: au-1-prod-cache
          passed:
            - notify-au-1-prod-demo-changes
          trigger: false
      - config:
        image_resource:
          source:
            repository: starkandwayne/concourse
            tag: latest
            type: docker-image
          inputs:
            - name: au-1-prod-changes
            - name: au-1-prod-cache
          outputs:
            - name: out
          params:
            BOSH_CA_CERT: |
              none
            BOSH_CLIENT: admin
            BOSH_CLIENT_SECRET: yepplease
            BOSH_ENVIRONMENT: http://127.0.0.1:25555
            BOSH_JOB_INTERRUPTIBLE: true
            CACHE_DIR: au-1-prod-cache
            CI_NO_REACT: 0
            CHURNER_JOB: au-1-prod
            GIT_BRANCH: master
            GIT_PROVIDER: github
            OUT_DIR: out/git
            PRUNING_JOB: au-1-sandbox
            VALDZ_ADR: laskhdfjaskdjlakdsjf
            VALDZ_ADR_IN: null
            VALDZ_SECRET: id: null
            VALDZ_SECRET_SECRET: null
            WORKING_DIR: au-1-prod-changes
        platform: linux
        run:
          args:
            - ci-pipeline-deploy
          path: au-1-prod-cache/.genesis/bin/genesis
        params:
          repository: out/git
        put: git
        task: conc-deploy
      - config:
        image_resource:
          source:
            repository: starkandwayne/concourse
            tag: latest
            type: docker-image
          inputs:
            - name: out
            - name: au-1-prod-cache
          outputs:
            - name: cache-out
          params:
            CI_NO_REACT: 0
            CHURNER_JOB: au-1-prod
            GIT_BRANCH: master
            GIT_PROVIDER: github
            OUT_DIR: cache-out/git
            WORKING_DIR: out/git
        platform: linux
        run:
          args:
            - ci-generate-cache
          path: au-1-prod-cache/.genesis/bin/genesis
          task: generate-cache
      - params:
          repository: cache-out/git
        put: git
        on_failure:
          do:
            - params:
                channel: slackjbaaskjhdfkj
                icon_url: http://ci.ly/image/3e1h0h3k2e0p/
              concourse-logo.png
            text: "cfsummit2018: Concourse deployment to
              au-1-prod-demo failed"
            username: runwaybot
            put: slack
            on_failure:
              do:
                - aggregate:
                  - params:
                      channel: slackjbaaskjhdfkj
                      icon_url: http://ci.ly/image/3e1h0h3k2e0p/
                    concourse-logo.png
                  text: "cfsummit2018: Concourse successfully
                    deployed au-1-prod-demo"
                    username: runwaybot
                put: slack
                public: true
                serial: true
            - name: au-1-sandbox-demo
              plan:
              - do:
                - aggregate:
                  - get: au-1-sandbox-cloud-config
                    trigger: true
                  - get: au-1-sandbox-runtime-config
                    trigger: true
                  - get: au-1-sandbox-changes
                    trigger: true
                  - get: au-1-sandbox-cache
                    passed:
                      - dev-demo
                    trigger: true
                  - config:
                    image_resource:
                      source:
                        repository: starkandwayne/concourse
                        tag: latest
                        type: docker-image
                      inputs:
                        - name: au-1-sandbox-changes
                        - name: au-1-sandbox-cache
                      outputs:
                        - name: out
                      params:
                        BOSH_CA_CERT: |
                          none
                        BOSH_CLIENT: admin
                        BOSH_CLIENT_SECRET: yepplease
                        BOSH_ENVIRONMENT: http://127.0.0.1:25555
                        BOSH_JOB_INTERRUPTIBLE: true
                        CACHE_DIR: au-1-sandbox-cache
                        CI_NO_REACT: 0
                        CHURNER_JOB: au-1-sandbox
                        GIT_BRANCH: master
                        GIT_PROVIDER: github
                        OUT_DIR: out/git
                        PRUNING_JOB: dev
                        VALDZ_ADR: laskhdfjaskdjlakdsjf
                        VALDZ_ADR_IN: null
```



JAMES HUNT

STARK & WAYNE

```
groups:
  - jobs
  - au-1-prod-demo
  - au-1-sandbox-demo
  - dev-demo
  - eu-1-prod-demo
  - eu-1-sandbox-demo
  - us-1-prod-demo
  - us-1-sandbox-demo
  - us-1-staging-demo
  - us-2-prod-demo
  - us-2-sandbox-demo
  - us-2-staging-demo
  - notify-au-1-prod-demo-changes
  - notify-eu-1-prod-demo-changes
  - notify-us-1-prod-demo-changes
  - notify-us-2-prod-demo-changes
name: cfsummit2018
jobs:
- name: notify-au-1-prod-demo-changes
  plan:
    - aggregate:
      - get: au-1-prod-changes
        trigger: true
      - get: au-1-prod-cloud-config
        trigger: true
      - get: au-1-prod-runtime-config
        trigger: true
      - get: au-1-prod-cache
        passwd:
          - au-1-sandbox-demo
        trigger: true
    - aggregate:
      - params:
          channel: slackjbaakjhdfkj
          icon_url: http://ci.ly/image/3e1h0H3K2e0P/
concourse-logo.png
      text: 'cfsummit2018: Changes are staged to be
        deployed to au-1-prod-demo.
        please schedule a run a deploy via Concourse'
        username: runwaybot
      put: slack
    public: true
    serial: true
- name: au-1-prod-demo
  plan:
    - do:
      - aggregate:
        - get: au-1-prod-changes
          passwd:
            - notify-au-1-prod-demo-changes
            trigger: false
        - get: au-1-prod-cache
          passwd:
            - notify-au-1-prod-demo-changes
            trigger: false
      - config:
        image_resource:
          source:
            repository: starkandwayne/concourse
            tag: latest
            type: docker-image
          inputs:
            - name: au-1-prod-changes
            - name: au-1-prod-cache
          outputs:
            - name: out
          params:
            BOSH_CA_CERT: |
              none
            BOSH_CLIENT: admin
            BOSH_CLIENT_SECRET: yepplease
            BOSH_ENVIRONMENT: http://127.0.0.1:25555
            BOSH_JOB_INTERRUPTIBLE: true
            CACHE_DIR: au-1-prod-cache
            CI_NO_REACT: 0
            CHURNER_JOB: au-1-prod
            GIT_BRANCH: master
            GIT_PROVIDER_JOB: nahaha
            OUT_DIR: out/git
            PRUNING_JOB: au-1-sandbox
            VALD_AUG: laskhdfjaskdjlakdsjf
            VALD_AUG_IN: null
            VALD_SECRET_ID: null
            VALD_SECRET_ID_SECRET: null
            WORKING_DIR: au-1-prod-changes
        platform: linux
        run:
          args:
            - ci-pipeline-deploy
            path: au-1-prod-cache/.genesis/bits/genesis
          params:
            repository: out/git
            put: git
            task: kosh-deploy
      - config:
        image_resource:
          source:
            repository: starkandwayne/concourse
            tag: latest
            type: docker-image
          inputs:
            - name: out
            - name: au-1-prod-cache
          outputs:
            - name: cache-out
          params:
            CI_NO_REACT: 0
            CHURNER_JOB: au-1-prod
            GIT_BRANCH: master
            GIT_PROVIDER_JOB: nahaha
            OUT_DIR: cache-out/git
            WORKING_DIR: out/git
        platform: linux
        run:
          args:
            - ci-generate-cache
            path: au-1-prod-cache/.genesis/bits/genesis
            task: generate-cache
      - params:
          repository: cache-out/git
          put: git
          on_failure:
            no_output:
              - params:
                  channel: slackjbaakjhdfkj
                  icon_url: http://ci.ly/image/3e1h0H3K2e0P/
concourse-logo.png
              text: 'cfsummit2018: Concourse deployment to
                au-1-prod-demo failed'
                username: runwaybot
          put: slack
        on_success:
          aggregate:
            - params:
                channel: slackjbaakjhdfkj
                icon_url: http://ci.ly/image/3e1h0H3K2e0P/
concourse-logo.png
                text: 'cfsummit2018: Concourse successfully
                deployed au-1-prod-demo'
                username: runwaybot
            put: slack
            public: true
            serial: true
- name: au-1-sandbox-demo
  plan:
    - do:
      - aggregate:
        - get: au-1-sandbox-cloud-config
          trigger: true
        - get: au-1-sandbox-runtime-config
          trigger: true
        - get: au-1-sandbox-changes
          trigger: true
        - get: au-1-sandbox-cache
          passwd:
            - dev-demo
          trigger: true
      - config:
        image_resource:
          source:
            repository: starkandwayne/concourse
            tag: latest
            type: docker-image
          inputs:
            - name: au-1-sandbox-changes
            - name: au-1-sandbox-cache
          outputs:
            - name: out
          params:
            BOSH_CA_CERT: |
              none
            BOSH_CLIENT: admin
            BOSH_CLIENT_SECRET: yepplease
            BOSH_ENVIRONMENT: http://127.0.0.1:25555
            BOSH_JOB_INTERRUPTIBLE: true
            CACHE_DIR: au-1-sandbox-cache
            CI_NO_REACT: 0
            CHURNER_JOB: au-1-sandbox
            GIT_BRANCH: master
            GIT_PROVIDER_JOB: nahaha
            OUT_DIR: out/git
            PRUNING_JOB: dev
            VALD_AUG: laskhdfjaskdjlakdsjf
            VALD_AUG_IN: null
```

SEVERAL.
THOUSAND.
LINES.
OF YAML.

A PIPELINE, IN 7 LINES.

```
auto dev-* *-sandbox-* *-staging-*
```

```
dev-demo -> au-1-sandbox-demo -> au-1-prod-demo
```

```
dev-demo -> eu-1-sandbox-demo -> eu-1-prod-demo
```

```
dev-demo -> us-1-sandbox-demo -> us-1-prod-demo  
           us-1-sandbox-demo -> us-1-staging-demo
```

```
dev-demo -> us-2-sandbox-demo -> us-2-prod-demo  
           us-2-sandbox-demo -> us-2-staging-demo
```



genesis repipe



JAMES HUNT

STARK & WAYNE

A detailed architectural wireframe of a city skyline, featuring various skyscrapers and buildings. The lines are thin and light gray, set against a dark blue background. The perspective is from a low angle, looking up at the buildings. The wireframe includes structural details like windows, balconies, and scaffolding.

GENESIS

DEMO

(CLOSE KEYNOTE, JAMES)



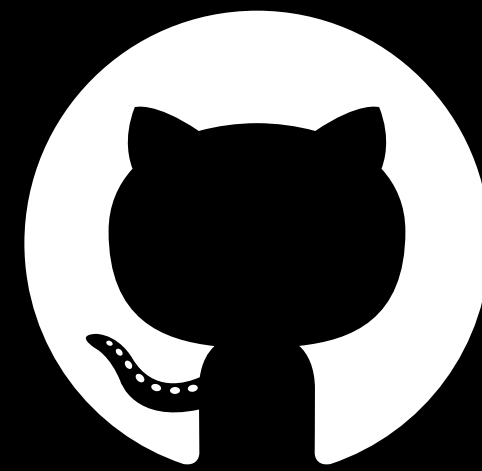
JAMES HUNT

(THEN OPEN UP TERMINAL)



JAMES HUNT

THANKS!



<https://github.com/genesis-community>
beahero@starkandwayne.com



JAMES HUNT