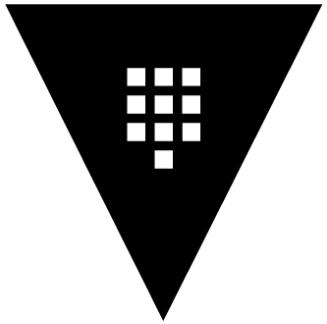
PADDYPOWER betfair



HashiCorp
Vault

Continuous Delivery Secrets Management with HashiCorp Vault

!@#$%^&*9

Secrets

Authentication | Authorization

- Usernames
- DB credentials
- API tokens
- TLS certificates

- source
- configuration management (chef, ansible, puppet)
- version control (github, gitlab)

HashiCorp Vault

OWASP Open Web Application Security Project

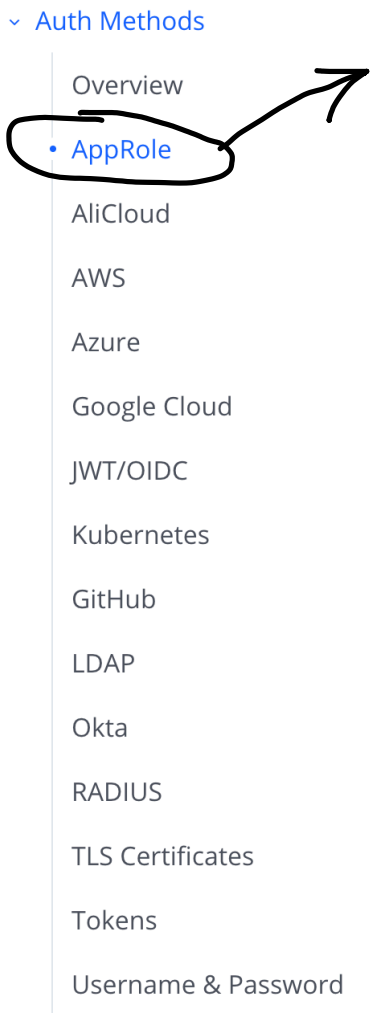
- Central
- Encrypt at rest/ in transit
- ACL
- Audit

```
# This section grants all access on "secret/*". Further restrictions can be
# applied to this broad policy, as shown below.
path "secret/*" {
  capabilities = ["create", "read", "update", "delete", "list"]
}

# Even though we allowed secret/*, this line explicitly denies
# secret/super-secret. This takes precedence.
path "secret/super-secret" {
  capabilities = ["deny"]
}
```

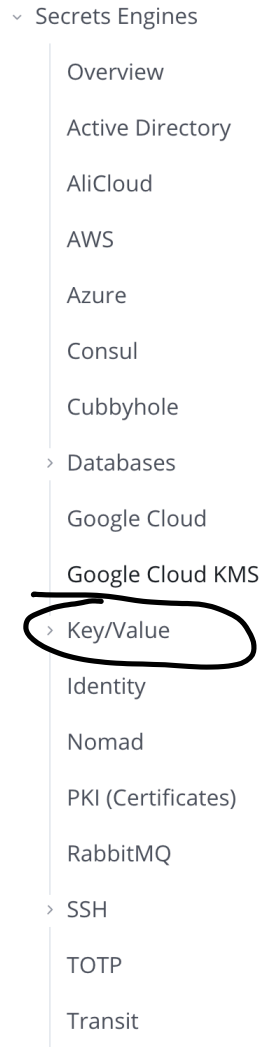
- Dynamic Secrets
  - Ephemeral
  - Unique
  - Revoke

Auth Methods and Secrets Engines



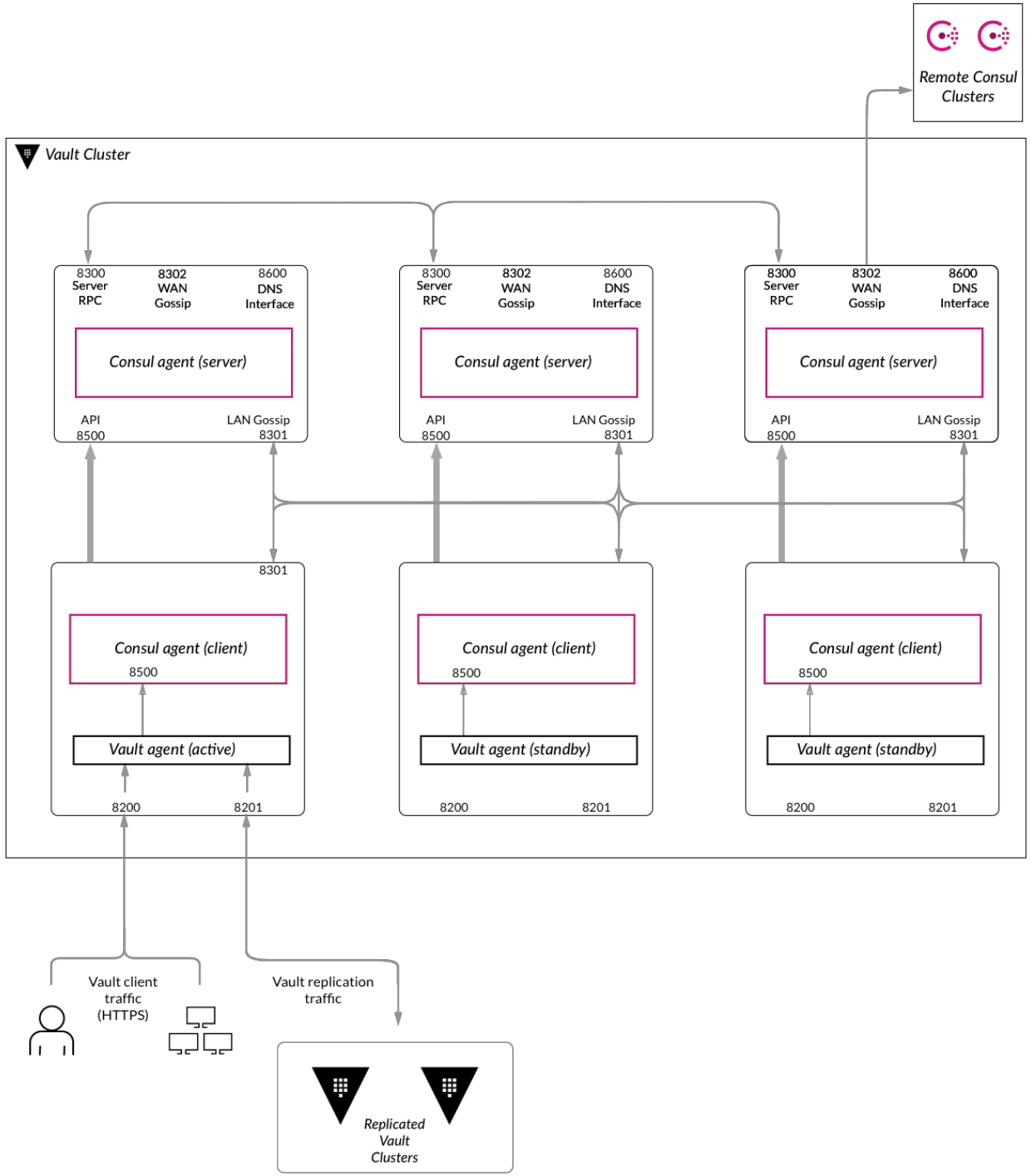
AppRole Definition

Method used by HashiCorp Vault for Secure Introduction. This is the process by which we can establish some level of trust to a system (server, node, container), such that we can share a token. That token can be used to then authenticate that system to Vault to allow for retrieval of secrets. The token can be scoped to a policy such that the system only has access to the relevant secrets for that system.



HashiCorp Vault

OWASP Open Web Application Security Project



Vault Architecture Reference diagram

Why?

* Vertical	Security
* Item	i2 secrets
* Group	Application
* Risk title	Insecure storage of i2 secret keys could lead to infrastructure compromise

production.rb 639 Bytes

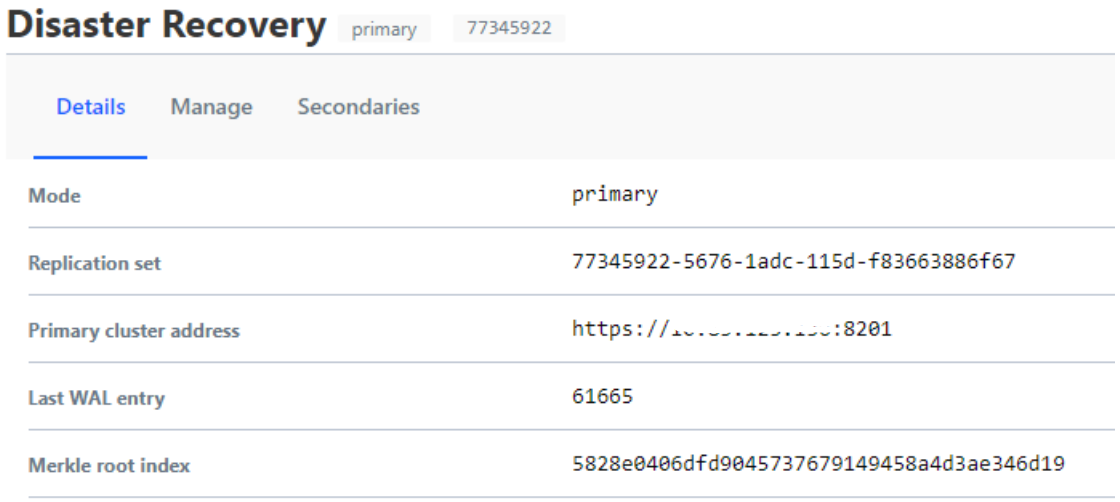
```
1  if node.chef_environment == '_production'
2          include_attribute "olympus::common"
3
4          default["oly"]["unicast_hosts"] = ["http://ie1-[illegible] prd.prd.
5          default["elasticsearch"]["host"] = "ol[illegible].betfair"
6
7          default["cname"] = "[illegible].betfair"
8          default["env"]   = "prod"
9
10         default["mysql_grafana"]["host"] = "[illegible]:3306"
11         default["mysql_grafana"]["user"] = "grafana_security_team"
12         default["mysql_grafana"]["password"] = "password01"
13         default["mysql_grafana"]["db"] = "grafana_security_team"
14 end
```

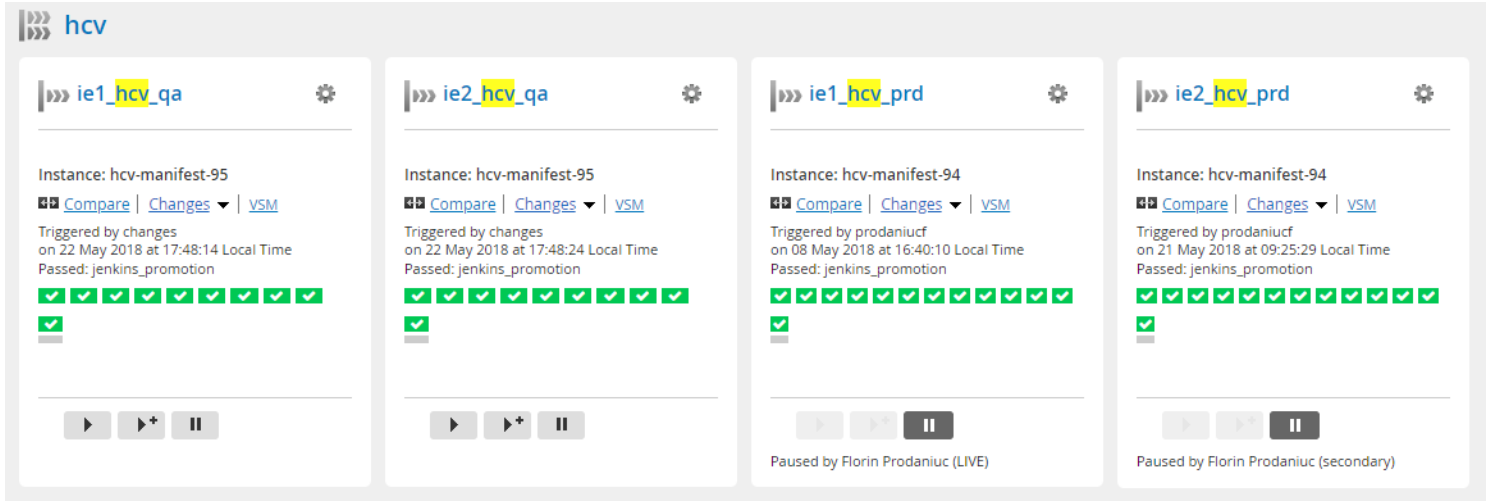
PADDYPOWER betfair

OWASP Open Web Application Security Project

What we did

Vault - Replication, Deployment





Scoping

J

jenkins_job_builder

[Data] Repository containing yaml files for jenkins jobs for tlas

SSH | git@gitlab.app.betfair:devops/jen

- **cm_scm_group:** Gitlab group where cookbooks/roles are stored

```
10    tla: "arc"
11    cm: "chef"
12    stable_tla: "arc"
13    cm_scm_group: "chef-cookbooks"
```

```
1  abc.yml,chef,abc,chef-cookbooks
2  abt.yml,chef,abt,chef-cookbooks
3  acw.yml,chef,acw,chef-cookbooks
4  afp.yml,chef,afp,chef-cookbooks
5  ahi.yml,chef,ahi,chef-cookbooks
6  ais.yml,chef,ais,chef-cookbooks
7  ala.yml,chef,ala,chef-cookbooks
8  ame.yml,chef,ame,chef-cookbooks
9  amt.yml,chef,amt,chef-cookbooks
10 ans.yml,chef,ans,chef-cookbooks
11 ansible_roles.yml,ansible,,ansible-roles
12 aos.yml,chef,aos,chef-cookbooks
13 app.yml,ansible,app,ansible-roles
```

Access Control for Users

Secure | https://gitlab.app.betfair/security/vault-access-control

GitLab Projects Groups More

README.md

Vault Access Control

Vault TLA-specific ACL

Do not change `service_now` entries in the YAML files as those are replaced on every refresh, use `manual` one to add people.

You can use emails or AD usernames in the lists.

There are 2 possible roles:

- `dev` : access to path `TLA/dev/*` and `TLA/common/*`
- `prd` : access to path `TLA/*` (hence including `TLA/prd/*`)

`service_now` users do not specify role as every user there will have `prd`. In `manual` item, roles should be specified below and users inside it.
Example with some `manual` entries:

```
- service_now:
  - Rick.Smith@mail.com
- manual:
  - prd:
    - doej
  - dev:
    - Jane.Martins@mail.com
```

Security › vault-access-control › **Repository**

master | vault-access-control / tlas / **afs.yml**

Updates from ServiceNow
AppSec Bot authored a month ago

afs.yml 187 Bytes

```
1  - service_now:
2    - [redacted]@blip.pt
3    - [redacted]@blip.pt
4    - [redacted]@blip.pt
5  - manual:
6    - prd:
7      - [redacted]@blip.pt
8  - groups:
9    - prd:
10     - Blip.BenHurOn
11     - MobDev
```

Sign in to Vault

Namespace / (Root)

Token | Username | LDAP | Okta | GitHub

Username

Password

More options

Sign In

Security › vault-access-control › Merge Requests › !570

Open | Opened about 3 hours ago by **AppSec Bot**

Service Now updates

Request to merge `servicenow_17_04_19_04_32_14` **into** `master`

Pipeline #125786 passed for 25ea0a10.

Merge | Remove source branch | Modify commit message

Chef/ Ansible Helpers

CHEF

Secure | https://gitlab.app.betfair/chef-cookbooks/vault/blob/master/libraries/default.rb

Projects Groups More

```
49      Chef::Log.info("==========================================")
50      Chef::Log.info("Vault: Your secrets were read successfully!")
51      Chef::Log.info("Vault: Your recipe should access the secrets from node.run_state['
52      node.run_state['vault-secrets'] ||= Hash.new
53      node.run_state['vault-secrets'][destination] = secrets
```

```
83  - default["mysql"]["password"] = "password01"
```

```
72  -         "password":"<%= node["mysql"]["password"] %>",
72  +         "password":"<%= secret()[:mysql_password] %>",
```

ANSIBLE

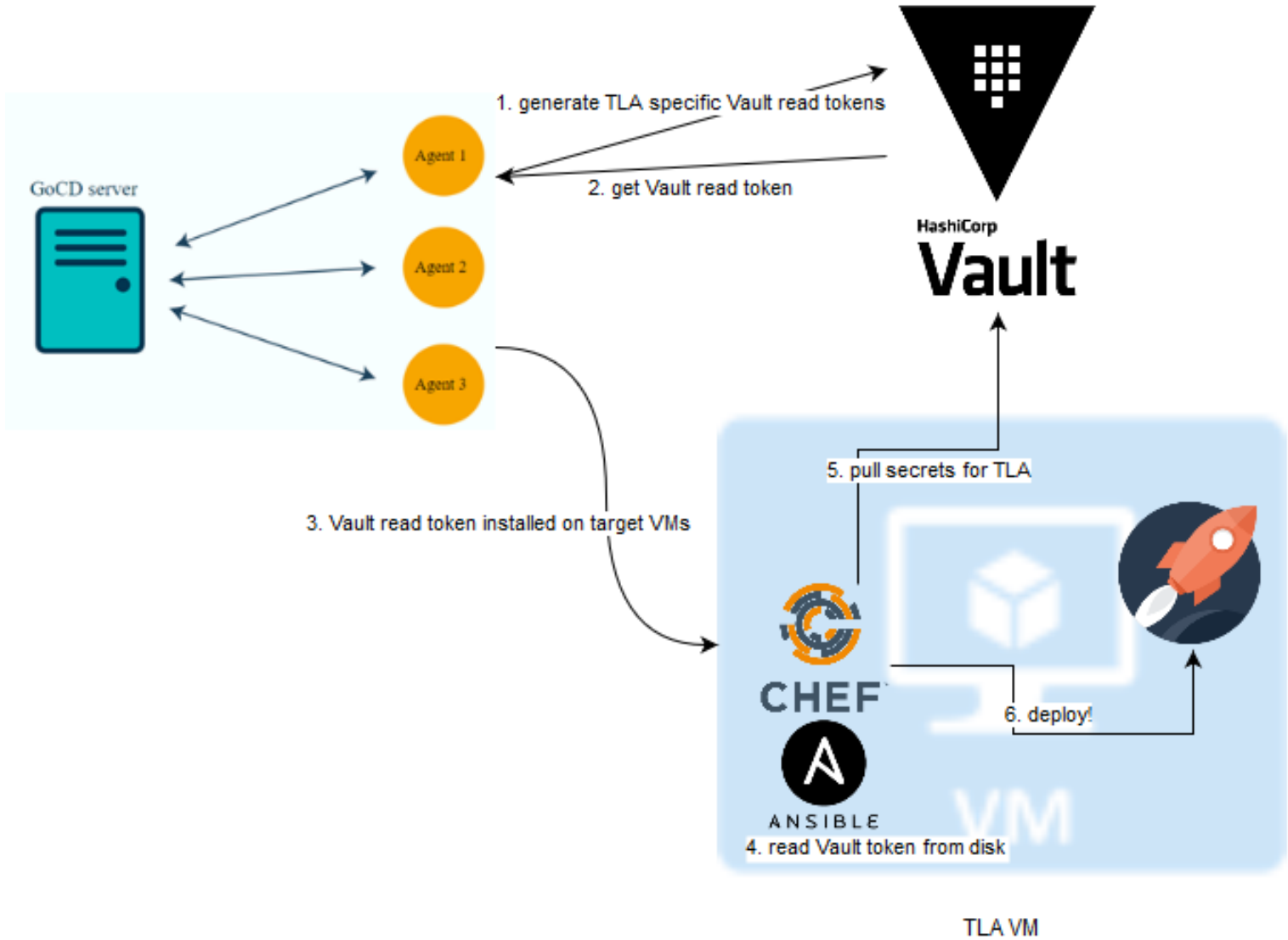
Secure | https://gitlab.app.betfair/devops/framework/blob/master/plugins/lookup/tla_secret.py

Projects Groups More

```
114     def load_path(self, path, ignore_cache=False, raise_invalid_path=True):
115         if path not in VAULT_CACHE:
116             display.vvvv('Retrieving secret at {}'.format(path))
117             data = self._vault_client.read(path)
```

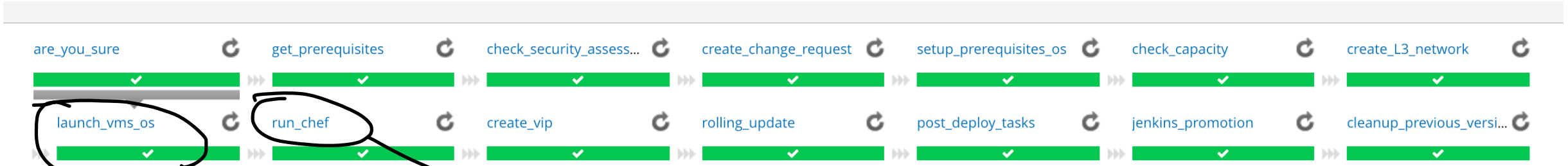
```
17  -   password: password01
```

```
21  -         'PASSWORD': '{{ database.password }}',
21  +         'PASSWORD': '{{ lookup('tla_secret')['database_password'] }}',
```


1. generate TLA specific Vault read tokens
2. get Vault read token
HashiCorp
Vault
GoCD server
Agent 1
Agent 2
Agent 3
3. Vault read token installed on target VMs
5. pull secrets for TLA
CHEF
6. deploy!
ANSIBLE
4. read Vault token from disk
VM

TLA VM

Pipeline integration



https://gitlab.app.betfair/devops/framework/blob/master/playbooks/launch_vms_os.yml

```
318      - include: "tasks/vault/generate_tla_read_token.yml"
```

Job Details | Pipeline ie1_oly_prd » Instance oly-manifest-310 VSM » Stage launch_vms_os / 1 » Job Launch_vms_os

Change theme

```
TASK [Generate token for tla] ***************************************************
task path: /go-agent/pipelines/ie1_oly_prd/playbooks/tasks/vault/generate_tla_read_token.yml:3
ESTABLISH LOCAL CONNECTION FOR USER: go
127.0.0.1 EXEC /bin/sh -c '( umask 22 && mkdir -p "` echo $HOME/.ansible/tmp/ansible-tmp-155483
mp-1554830052.82-125987472843321 `" )'
127.0.0.1 PUT /tmp/tmpdvV1Kq TO /home/go/.ansible/tmp/ansible-tmp-1554830052.82-125987472843321
127.0.0.1 EXEC /bin/sh -c 'LANG=en_GB.UTF-8 LC_ALL=en_GB.UTF-8 LC_MESSAGES=en_GB.UTF-8 /usr/bin
1/vault_generate_tla_token; rm -rf "/home/go/.ansible/tmp/ansible-tmp-1554830052.82-12598747284
ok: [ie1-oly01-prd.prd.betfair -> 127.0.0.1] => {"censored": "the output has been hidden due to
No logs from this task due to the fact that 'no_log: true' was specified for this result.
```

Berksfile 665 Bytes

```
1  source "http://berkshelf.dev.betfair"
2
3  # Helper method
4  def chef_cookbook(name, options = {})
5   cookbook(name, {
6     git: "git@gitlab.app.betfair:chef-cookbooks/#{name.downcase}.git"
7   }.merge(options))
8  end
9
10 metadata
11 chef_cookbook 'yum', branch: 'master'
12 chef_cookbook 'yum_app_betfair', branch: 'master'
13 chef_cookbook 'yum_package_verify', branch: 'master'
14 chef_cookbook 'yum_cleaner', branch: 'master'
15 chef_cookbook 'loghandle-mock', branch: 'master'
16 chef_cookbook 'sensu', branch: 'master'
17 chef_cookbook 'tsdb', branch: '3.3.0'
18 chef_cookbook 'splunkcollector', branch: 'master'
19 chef_cookbook 'rsyslog-client', branch: 'master'
20 chef_cookbook 'vault', branch: '1.0.0'
```

PADDYPOWER betfair

OWASP Open Web Application Security Project

Documentation

tfair/display/InfoSec/Vault+TLA+On-boarding+Guide#VaultTLAOn-boardingGuide-Chef

Calendars Create ...

Read the secrets from Vault:

Add dependency cookbook

metadata.rb

```
depends "vault"
```

Point to it in the Berksfile

Berksfile

```
# avoid using 'master' here as this branch can change
# choose a branch version (1.0.0, 2.0.0, ...) to be sure your deploy remains stable
# check available branch versions here https://gitlab.app.betfair/chef-cookbooks/vault
chef_cookbook 'vault', branch: '<choose your branch wisely>'
```

Include the helper class under the template in recipes, for example:

/recipes

```
template '/etc/grafana/grafana.ini' do
  ...
  helpers(VaultHelper)
end
```

Read the secrets as needed

Secrets can be accessed under /templates, using the following:

/templates

```
"my_password": "<%= secret()[:x_password] %>" # provided that the deploy is in QA and x_password is stored at /tla_name/qa
```

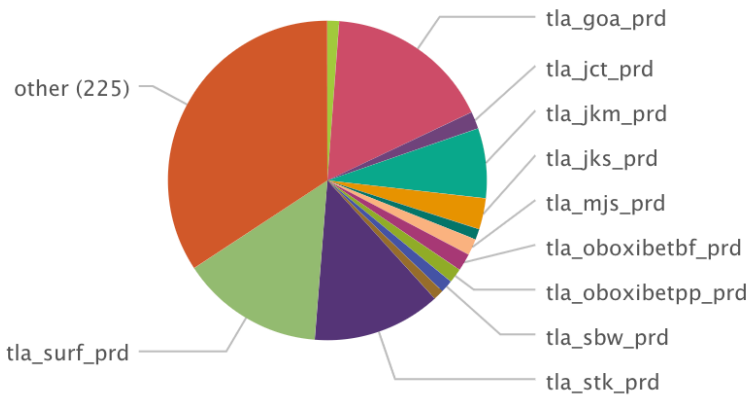
Stats

New Search

```
index="security-shared" host=*hcv* sourcetype="vault-audit" "request.operation"=read "request.path"="tla*" "type"=response "auth.metadata.role_name"="*prd"
| stats count by auth.metadata.role_name
```

✓ 29,191 events (3/16/19 3:37:36.000 PM to 4/15/19 3:37:36.000 PM) No Event Sampling Job

secrets requests - last 30 days




```
index=* host=* sourcetype="vault-audit" "type"=request "request.operation"=* | stats count by request
    .operation
```

Last 1 day

✓ 81,472 events (4/15/19 7:45:22.000 AM to 4/16/19 7:45:22.000 AM) No Event Sampling Job Fast Mode

Events | Patterns | Statistics (5) | Visualization

20 Per Page Format Preview

request.operation	count
read	76942
update	4139
list	343
create	42
delete	6

PADDYPOWER betfair

OWASP Open Web Application Security Project

Credits

Florin Prodaniuc

Filipe Pina

Alexandru Dima

Cristian Iaroi

```
for name in [
        'Teo',
        'Duarte',
        'Michael Ashe (Cloud Automation)',
        'Federico Prando (Cloud Automation)',
        'a bunch of developers for feedback and PoC-ing',
        others_missed
]:
        special_thanks(name)
```

HashiCorp Vault

PADDYPOWER betfair

OWASP Open Web Application Security Project

Learning Resources

- https://learn.hashicorp.com/
- https://www.katacoda.com/learn?q=vault
- download binary and just `vault server -dev`

More info?

/alexandrudima

HashiCorp Vault