📅 Feb 27, 2020 5:00 pm - 8:00 pm EDT

Exploring Ansible and OpenShift 4 Integrations for the Enterprise

📍 The Dineen Lounge - iQ Venues 140 Yonge St, Lower Level, Toronto, ON M5C 1X6

- Christopher
  - Current life as Consultant @ Arctiq Inc
  - Former teacher at Seneca College
  - Boxing, Yoga, Volleyball
  - Love learning new languages
  - 7 years in Linux/sysadmin/open source space
  - Red Hat kickstarted my career

Terraform

- **(Remote) state files**
- **Infra provisioning**
- **Provider/provisioner**
- **Implicit dependencies**
- **Specialised**
- **Declarative**
- **Idempotent**

Ansible

- **Inventories**
- **Config management**
- **Modules**
- **Sequential operations**
- **Jack of all trades**
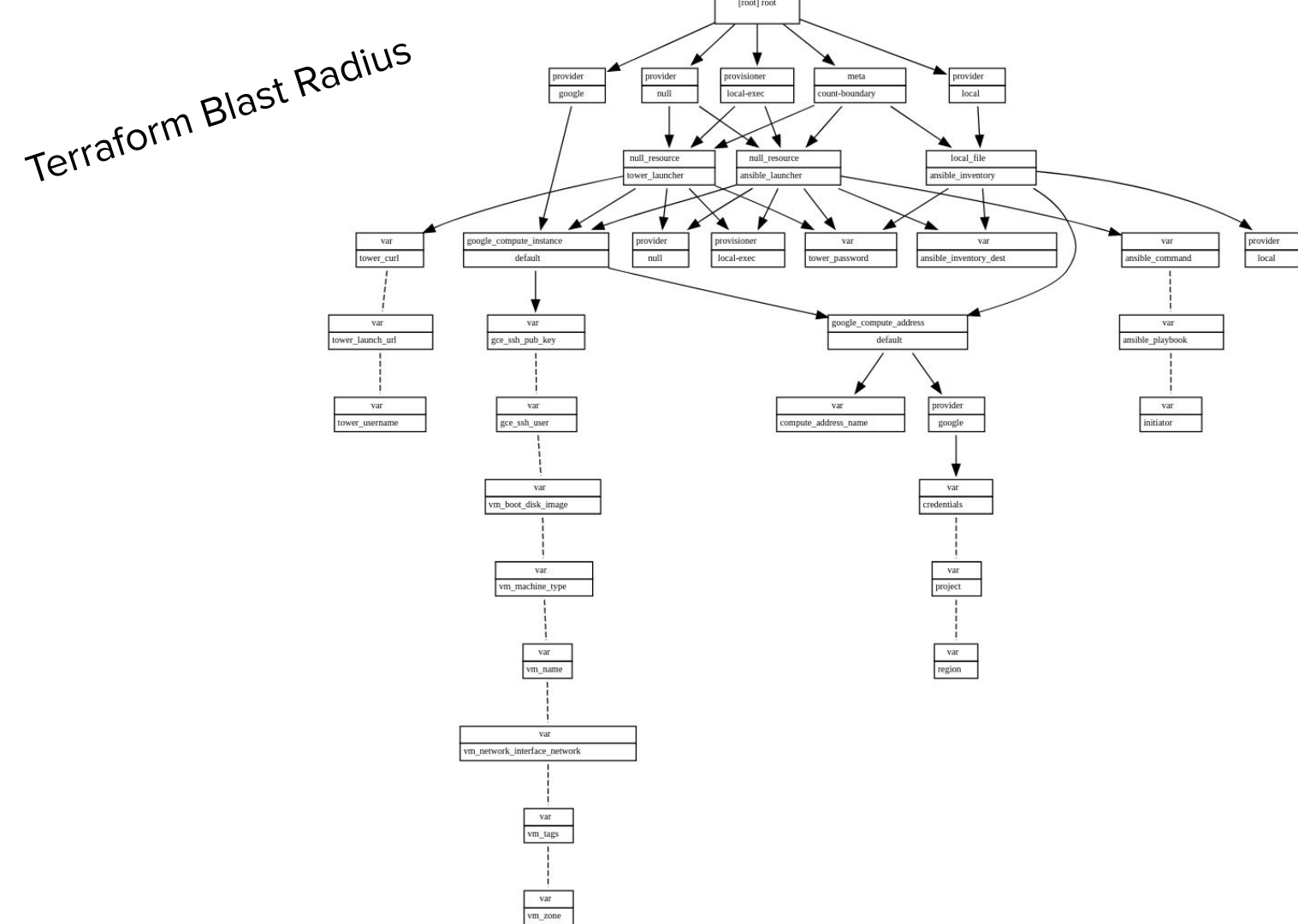- **Declarative**
- **Idempotent**

// Use the right tool for the job

Terraform

- Spinning up and tearing down resources is simple and fun.
- Don't rely on **local-exec** too much.

Ansible

- Configure all of the things!
- Rolling back infrastructure can be a dependency nightmare.

Terraform Blast Radius

```
{% for vms in terraform_vms %}
variable "vms_{{ vms['group'] }}" {
  default = [
  {%    for vm in range(vms['count']) %}
  {%      if loop.index < 10 %}
    "{{ vms['naming'] }}-0{{ loop.index }}.{{ vsphere_pri_domain_name }}",
  {%      elif loop.index >= 10 %}
    "{{ vms['naming'] }}-{{ loop.index }}.{{ vsphere_pri_domain_name }}",
  {%      endif %}
  {%    endfor %}
  ]
}
{% endfor %}
```

Arctiq
INTELLIGENT ARCHITECTURE

adammck / **terraform-inventory**

👁 Watch ▾ | 55 | ★ Star | 1.3k | ⑂ Fork | 233

<> Code | ⓘ Issues 42 | Pull requests 10 | ▶ Actions | 🛡 Security | Insights

Terraform State → Ansible Dynamic Inventory

go | ansible | terraform

🕐 **149** commits | ⑂ **1** branch | 📦 **0** packages | 🏷 **13** releases | 👥 **45** contributors | ⚖ MIT

● **Go** 97.3% | ● **HCL** 1.6% | ● **Shell** 1.1%

Branch: **master** ▾ | **New pull request** | | Create new file | Upload files | Find file | Clone or download ▾

🧔 **karras** Support OTC metadata parsing (#141) | ✓ Latest commit `c7e468f` 5 days ago

📁 bin | Fix deprecation warning | 4 years ago
📁 fixtures | Add vSphere IP location (#67) | 3 years ago
📁 pkg | Add bin/dist | 5 years ago

Demo Time!

- Tower Job Schedules
- Multiple (Smart) inventories with filtering
- Terraform/Ansible pre-commit hook validation

github.com/Markieta

arctiq.ca/our-blog

Arctiq

INTELLIGENT ARCHITECTURE

- Aaren
  - Current life as Consultant @ Arctiq Inc
  - Over 16 years in I.T.
  - Prior life as Audio Engineer
  - Husband & a father of 2 little girls
  - Open-source reborn after a Windows upbringing
  - Tesla enthusiast
  - Avid 'home-labber'

- Version 4**.3**
- UI has been improved
- *IPI* currently for Azure, AWS, GCP, RHOSP13 and RHOSP16
- *UPI* for VMware, BareMetal, RHV, IBM Z and IBM LinuxOne
- Support for FIPS crypto
- OCS 4.2 (Ceph) + various other storage add's

- Private cluster networking options!
  - IPI into existing subnet & VPC/VNet on big3 clouds
- Encrypt ETCD data.. encrypted secrets!
- Log forwarding outside cluster (Tech Preview)
- Helm integration (Tech Preview)
- Numerous other additions & bug fixes

Or, in other words, understanding the CRDs used by the machine-config operator, and the benefits of oc CLI for machine debug 😉
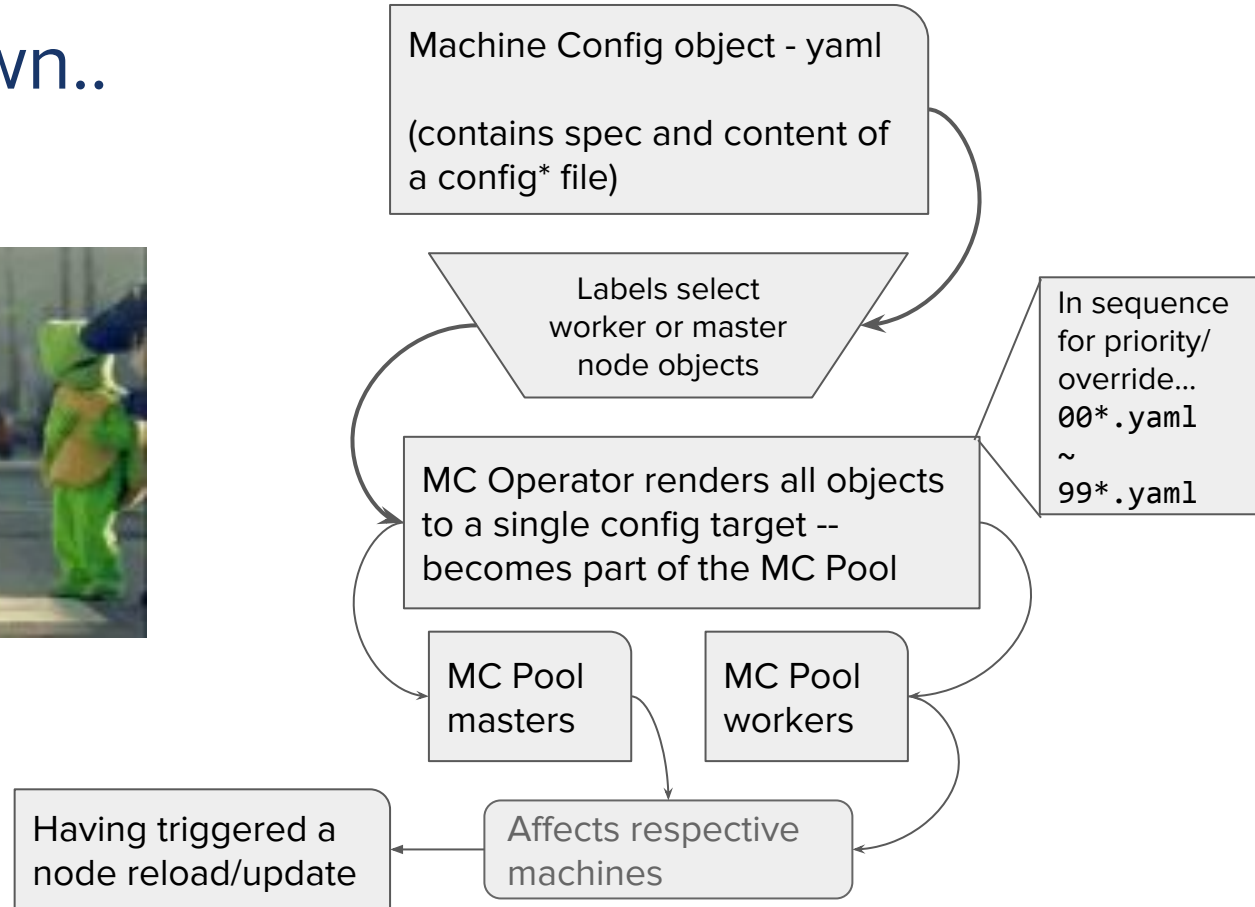
Why Do This?

- Alter node system configs in a k8s native way
  - Secured by OCP RBAC, auth, security
  - Node config as code artifacts! IaC!
  - Let the Operator do its job!
- We don't do node OS CLI
  - * demo with SSH
- We don't want humans with direct node OS access!

Let's Break it Down..

Machine Config object - yaml

(contains spec and content of a config* file)

Labels select worker or master node objects

In sequence for priority/override…
`00*.yaml` ~ `99*.yaml`

MC Operator renders all objects to a single config target -- becomes part of the MC Pool

MC Pool masters

MC Pool workers

Having triggered a node reload/update

Affects respective machines

Special Guest: **Infra Nodes**

- Remember those guys?!
- We *can* have them in OCP4!
- For Monitoring, Logging, Router, Registry!
- It's a bit involved (no demo), but doable!
- We would setup Infra type *MachineSets*
- Which is a great segway to..
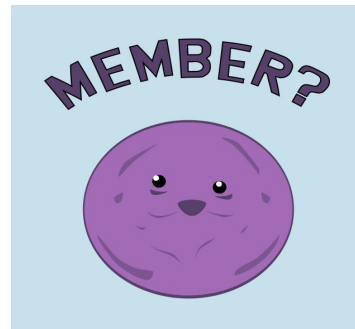
MachineSets

- *Not the same as Machine Config Pools*
- MCPs are groups of common function nodes
- MachineSets are scalable groups of similar compute-type nodes
- Can be scaled automagically by the MachineAutoscaler and ClusterAutoscaler

MachineSets

- *Define things like*
  - Labels
  - cloud/infra Instance type/size
  - Block storage
  - Replica count (number of machines!)

Machine Config Pool

- *manages node cluster Machine Configs*
- Configs such as
  - Node registry access
  - Node capability configs (eg: GPU specifics)
  - Node storage or cri-o configs
  - Garbage collection settings

Machine Config (File) Change Demo

MachineSet Scaling Demo

CoreOS Node Debug Demo

Q&A

arctiq.ca/our-blog

learn.openshift.com

Arctiq
INTELLIGENT ARCHITECTURE

Up Next..

//Who is this?

- Hart
  - Current life as Consultant @ Arctiq Inc
  - Infrastructure and Networking background
  - Fan of sporting and live events
  - Much of life is spent with my 2 kids and various days and nights in arenas and soccer fields
  - Continuously learning

- Ansible Tower

- HashiCorp Vault

- GitHub (source code management)

- Webhook
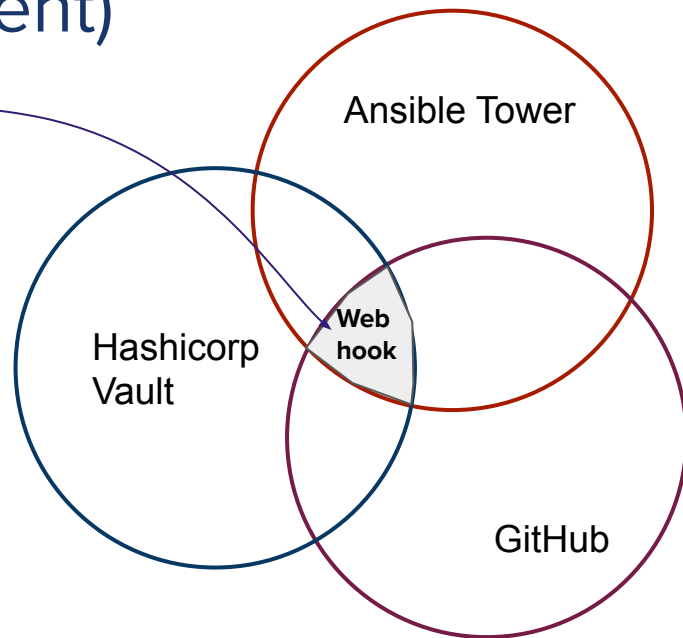
Why Integrate? ... Better Together

- Ansible Tower ➜ HashiCorp Vault for secrets/keys/certs
- Allows security team to be responsible for credential vault/access policies/roles
- Ansible Tower for orchestration leveraging RBAC/workflows/configuration management
- Keys/Passwords are stored and managed centrally

Ansible Tower with HashiCorp Vault Secrets Engine

- Extend the existing Ansible Tower encrypted credential store
  - Support other tools/integration (purpose-built) and best-of-breed
- Secure, versioned credentials (history)
- Centralized security strategy
- Security audit logging in Vault

Ansible Tower

- Git Workflows with Webhook Integration

- Ansible Tower now has built-in Webhook capabilities in Job Templates!
- Uses PAT and supports GitHub and GitLab atm
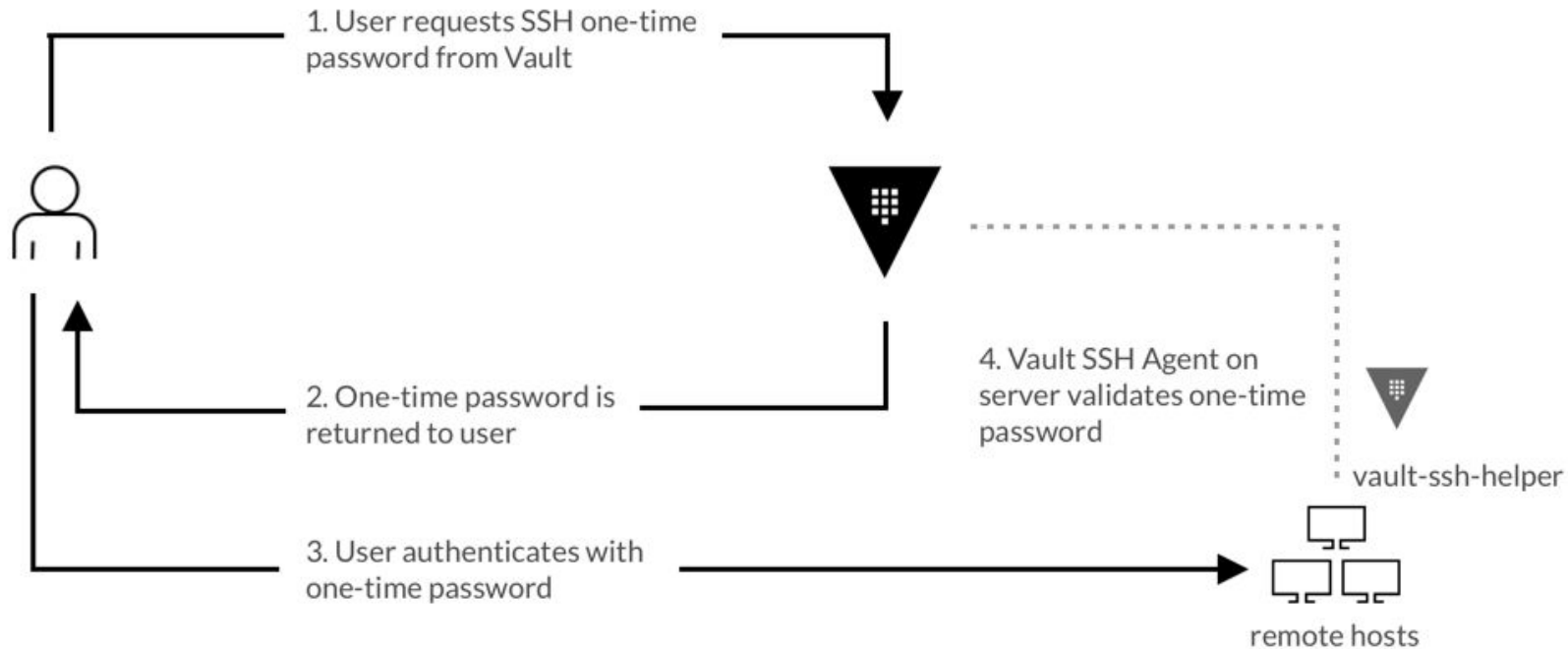- Calls the Tower API when code is pushed to the SCM repository

Ansible Tower

- Git Workflows with Webhook Integration

- Highlight the Ansible Tower API capabilities
- Use Git as centralized approval workflow for code
- Easily rollback/revert
- Branch protection/PR Workflow/Slack Notification
- IaC
- No credentials in Git!

Demo Time!

Ansible Tower - Dynamic SSH Secrets

- Bye! Bye! to the copy and pasting of credentials... updates/username/passwords ERROR PRONE!!
  - Centralized AND secure management of secrets
- Remote device authentication and management using Vault issues OTP/credentials
- TLS between Ansible Tower and Vault
- Bootstrapping

1. User requests SSH one-time password from Vault

2. One-time password is returned to user

3. User authenticates with one-time password

4. Vault SSH Agent on server validates one-time password

vault-ssh-helper

remote hosts

Demo Time!

THANK YOU!!!