# Linux Conf Australia 2017 - Hobart
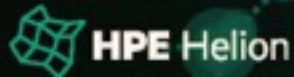
Running Production Workloads in a Programmable Infrastructure
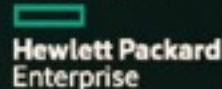
Alex Tesch
Cloud Consultant
Alejandro.tesch@hpe.com

HPE Helion

Accelerating next

Hewlett Packard Enterprise
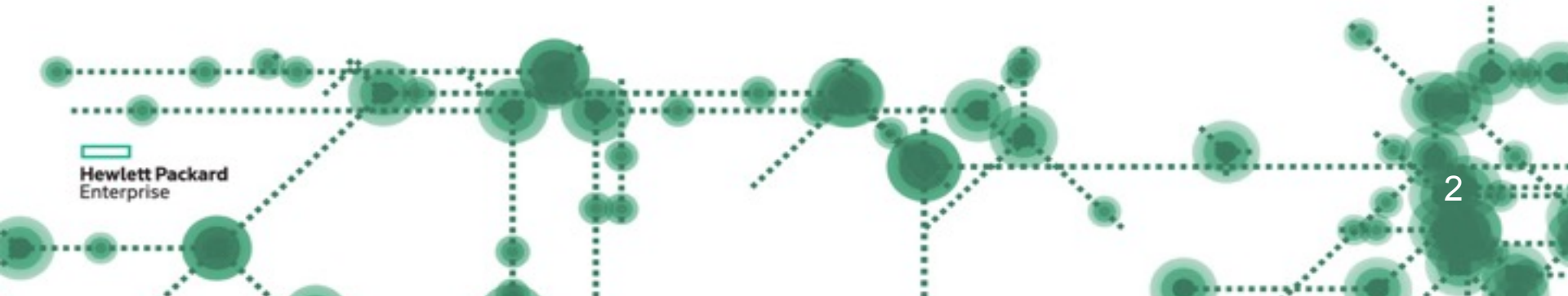
Advanced OpenStack use cases
What will we cover ?

– Orchestration for a Two-Tier environment

– LBaaS

  – Proactive auto Scaling

– FWaaS

  – Dynamic security

– Data cloning as a service
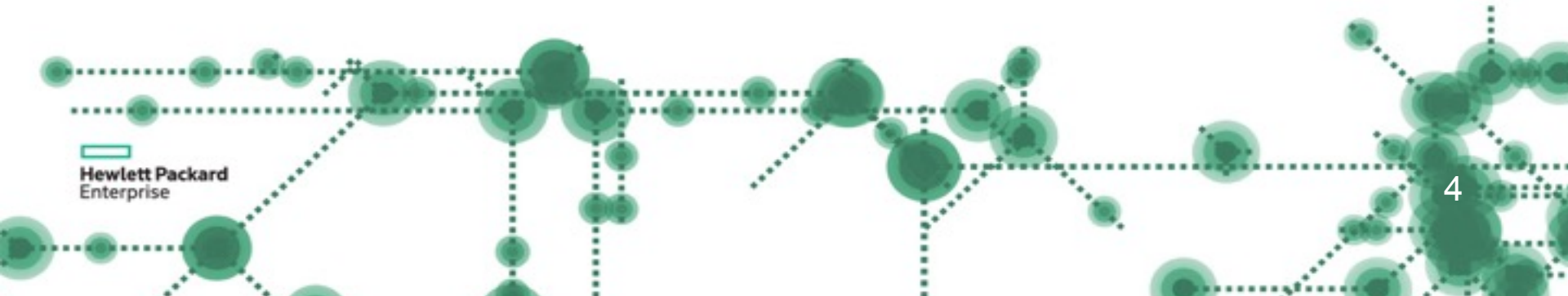
Live OpenStack Use Case Demos
4 Live Demos… What could possibly go wrong????
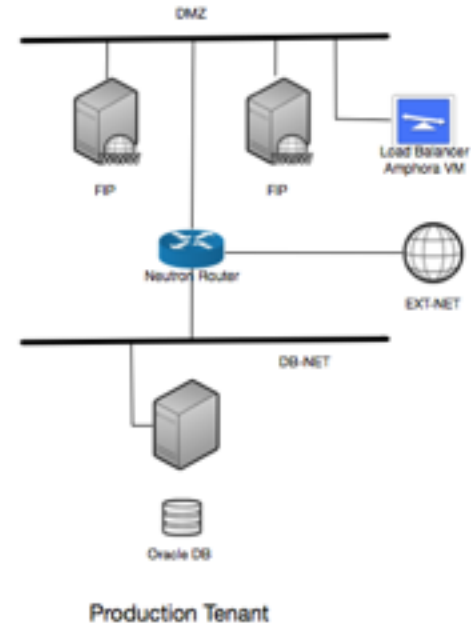
Orchestration Demo
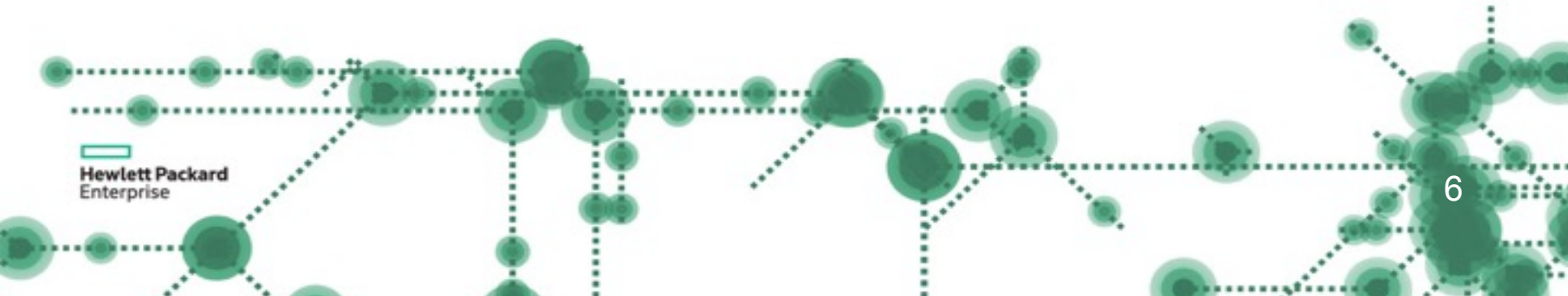
What we will build

– A DMZ Network with two Tomcat servers and a Load Balancer

– A DB Network with an Oracle Server attached to a Cinder Volume

– A Neutron Router to allow access from EXT-NET to the app

Production Tenant
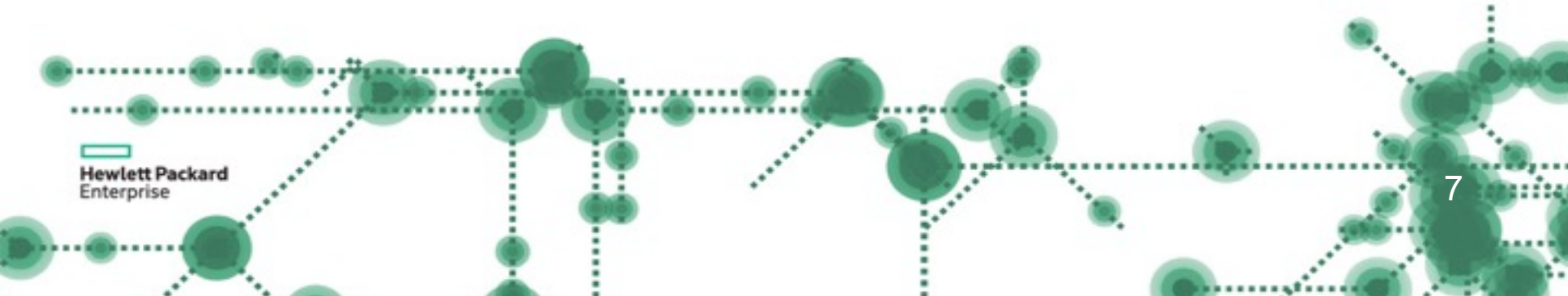
LBaaS

Load Balancer as a Service

Load Balancer as a Service

– Auto scaling via threshold

– Variety of load balancers supported (Amphoras, Kernel NS, F5, etc)

– Control load balancers by code

Hewlett Packard
Enterprise
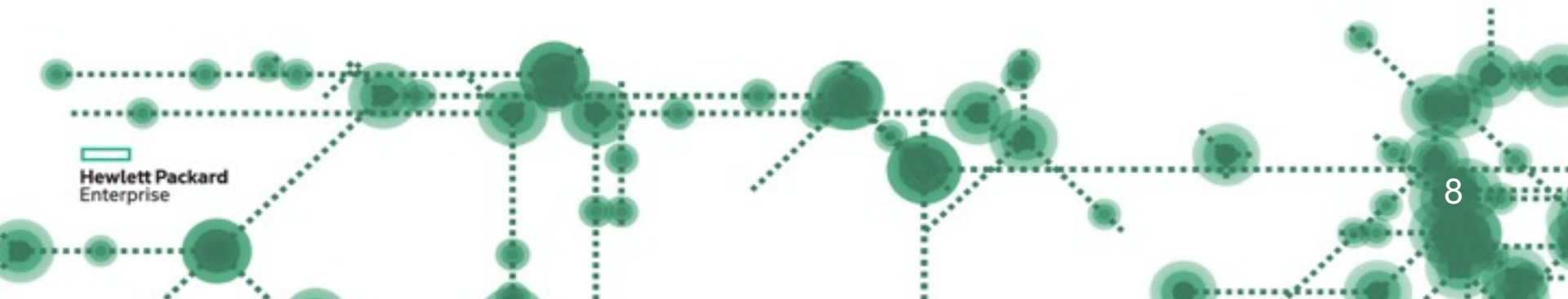
Current Neutron Limitations
How do we overcome them?
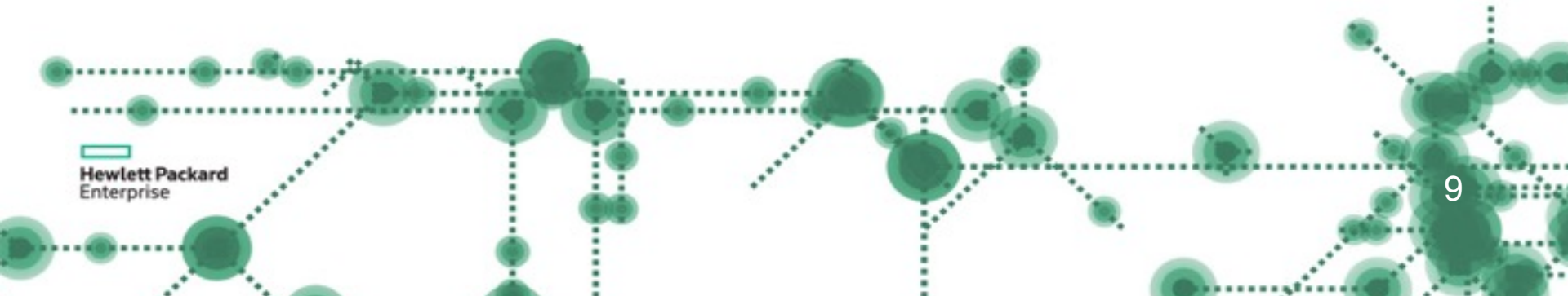
LBaaS v2 Limitations in current enterprise distros

– No HA capabilities for LBaaS v2 control plane

  – Although the Data Plane HA has been addressed with Octavia in the Mitaka Release (we can loose an amphora in the group and HAproxy will continue to work on the next available amphora)

  – Loosing the Neutron Controller running the LBaaS controlplane will hinder the LBaaS functionality.

Hewlett Packard
Enterprise

8
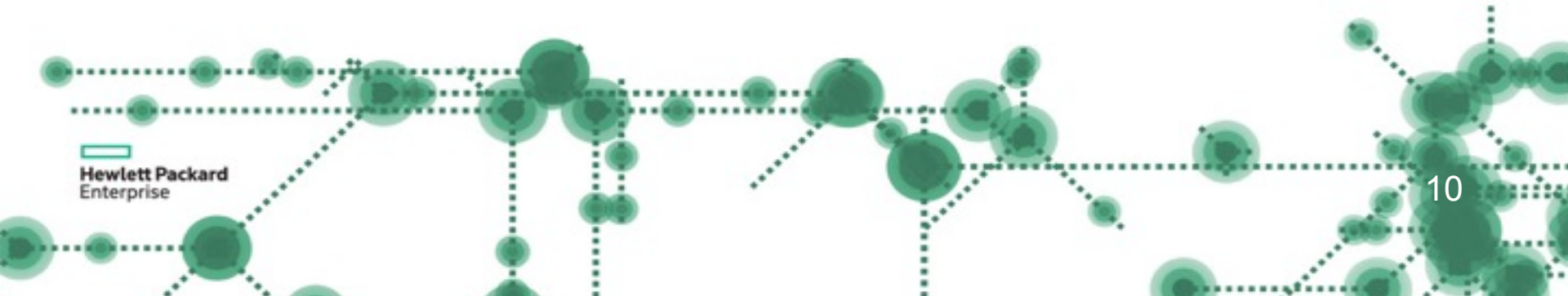
LBaaS / Autoscaling demo

FWaaS

Fire Wall as a Service

Hewlett Packard
Enterprise
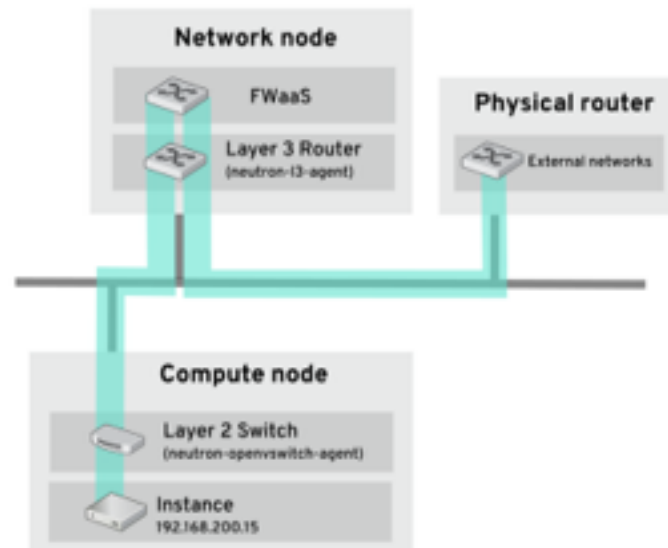
Firewall as a Service

FWaaS key take aways:

• The Firewall-as-a-Service (FWaaS) plug-in adds perimeter firewall management to OpenStack Networking (neutron).

• FWaaS Supports one firewall policy and logical firewall instance per project.

• FWaaS operates at the perimeter by filtering traffic at the OpenStack Networking (neutron) router. This distinguishes it from security groups, which operate at the instance / OpenVSwitch level.

• The example diagram on the right illustrates the flow of ingress and egress traffic for the VM2 instance

11
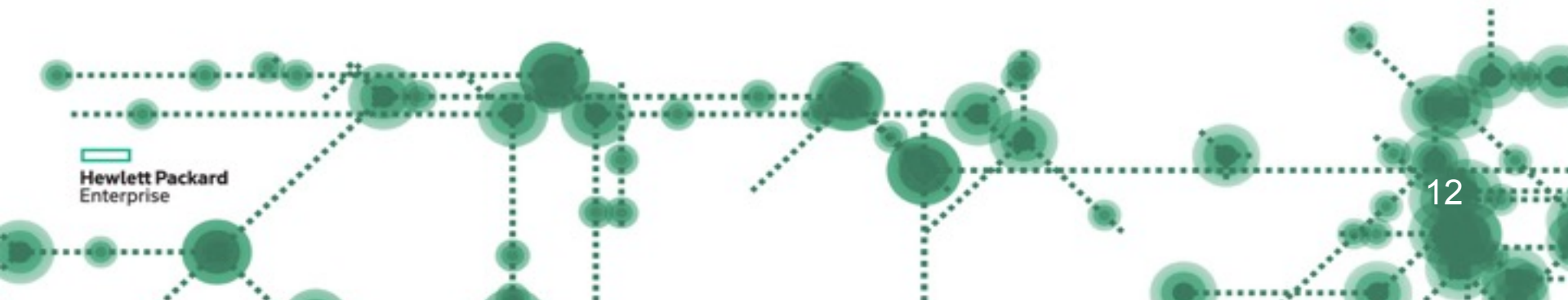
Firewall as a Service

FWaaS key take aways:

• FWaaS uses iptables to apply firewall policy to all virtual routers
within a project.

```
[root@hos case3[keystone_db]]# ip netns exec qrouter-57b3a5d6-10ea-4d83-9440-03f16bca7d7c iptables -L |grep icmp
DROP         icmp --  anywhere             anywhere
DROP         icmp --  anywhere             anywhere
DROP         icmp --  anywhere             anywhere
DROP         icmp --  anywhere             anywhere
[root@hos case3[keystone_db]]#
```

Hewlett Packard
Enterprise
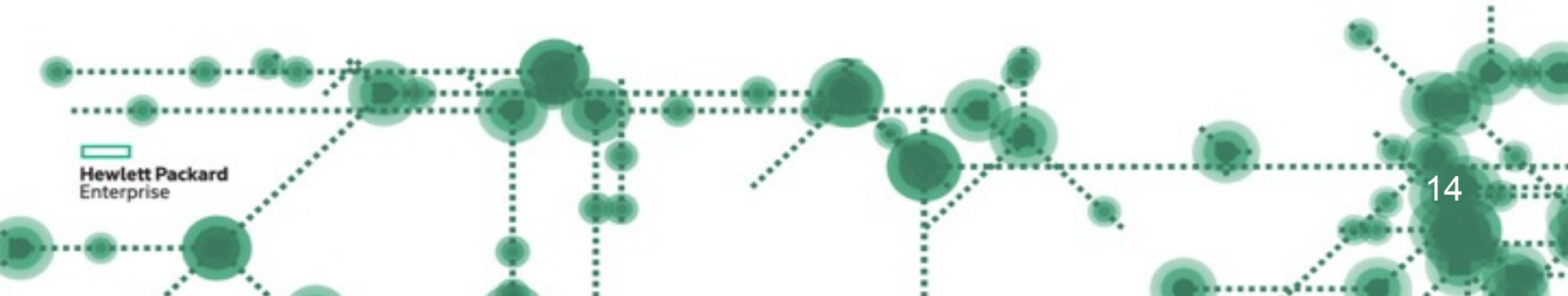
Firewall as a Service

Security Group key take aways:

• They are implemented in the OpenvSwitch layer (L2) and enforced by iptables in the ovs port for the instance

```
[root@hos neutron]# iptables -S |grep 1521
-A neutron-openvswi-i775324aa-b -p tcp -m tcp --dport 1521 -j RETURN
-A neutron-openvswi-ie985d409-1 -p tcp -m tcp --dport 1521 -j RETURN
[root@hos neutron]# iptables -S |grep 22
-A neutron-openvswi-i7901eaba-0 -p tcp -m tcp --dport 22 -j RETURN
-A neutron-openvswi-i946c2861-6 -p tcp -m tcp --dport 22 -j RETURN
-A neutron-openvswi-ie985d409-1 -p tcp -m tcp --dport 22 -j RETURN
[root@hos neutron]# iptables -S |grep 8080
-A INPUT -p tcp -m multiport --dports 8080 -m comment --comment "001 swift proxy
  incoming swift_proxy" -j ACCEPT
-A neutron-openvswi-i7901eaba-0 -p tcp -m tcp --dport 8080 -j RETURN
-A neutron-openvswi-i946c2861-6 -p tcp -m tcp --dport 8080 -j RETURN
-A neutron-openvswi-ie985d409-1 -p tcp -m tcp --dport 8080 -j RETURN
[root@hos neutron]#
```

Hewlett Packard
Enterprise
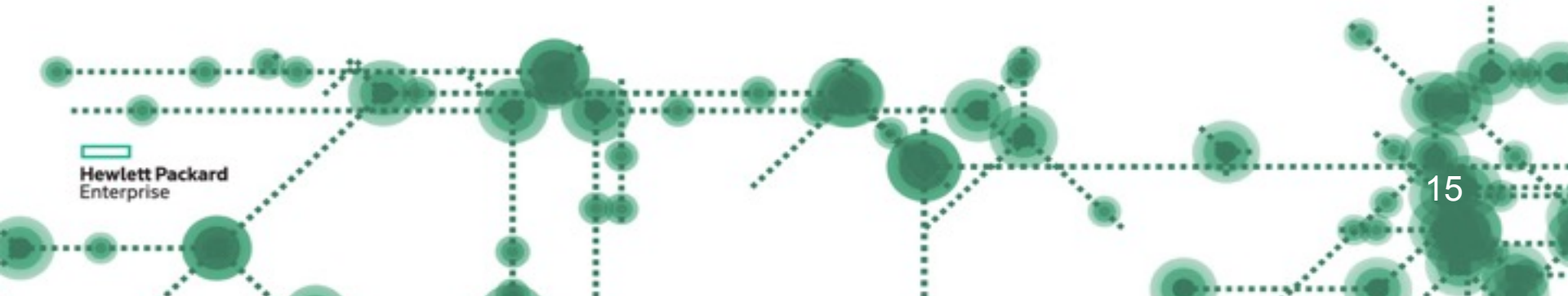
# FWaaS Demo
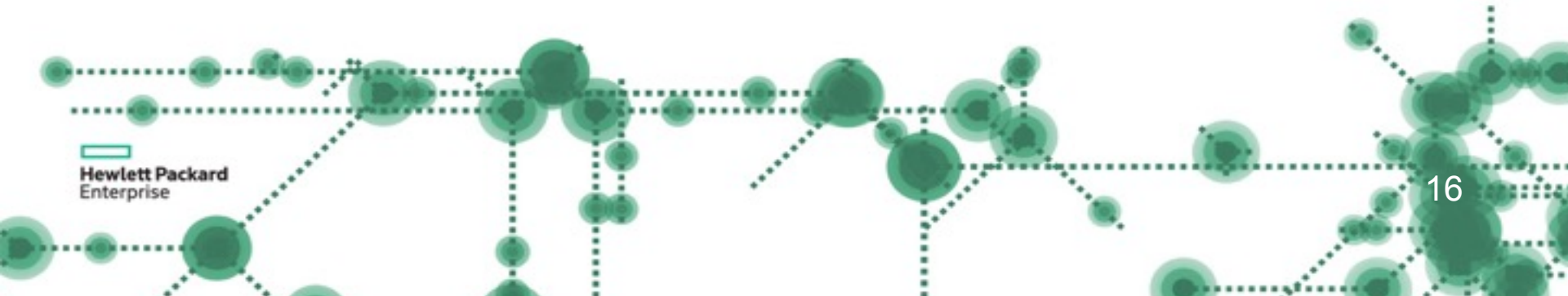
Data Cloning as a Service

Developers can now make use of the latest production data to run their tests.
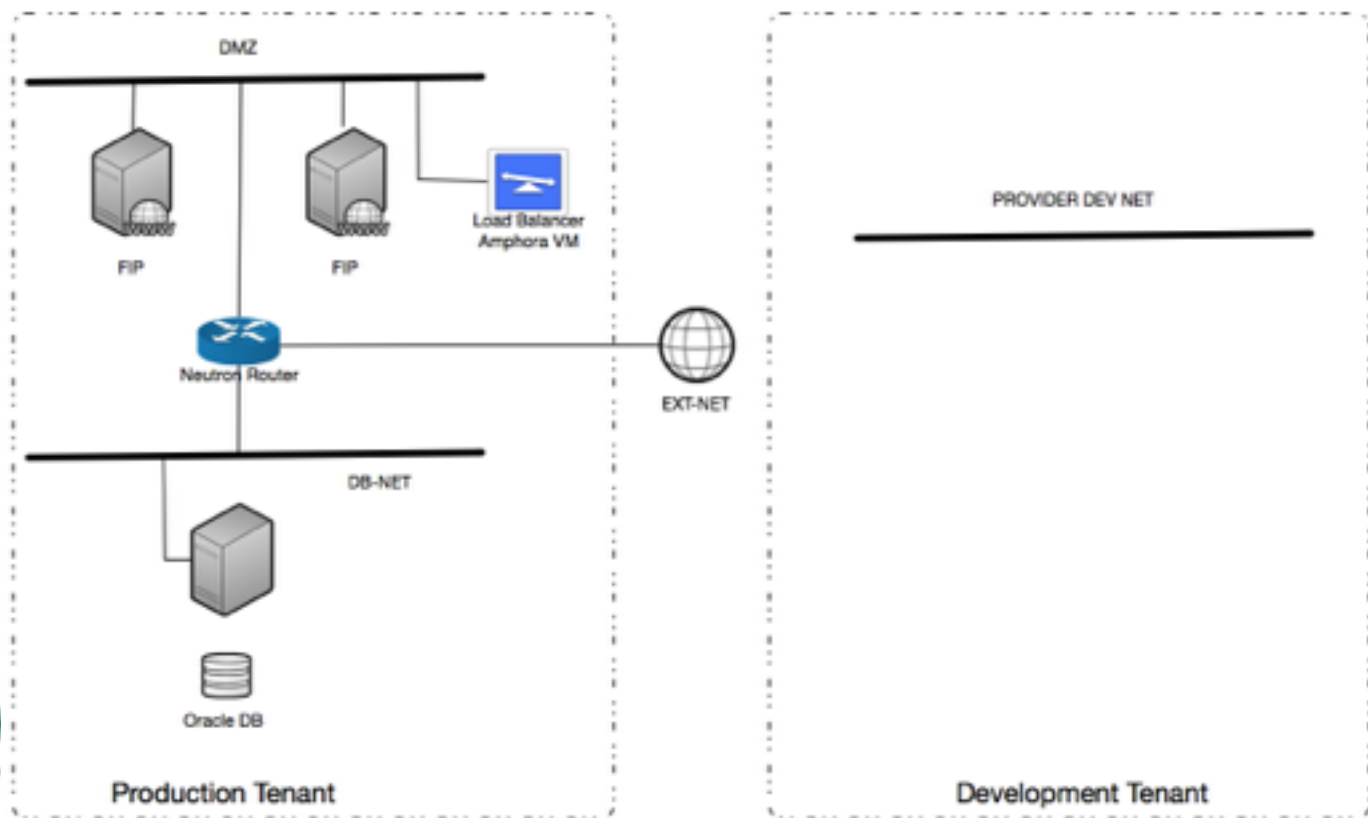
– Since the Oracle server is under OpenStack control, fully automating the database cloning by code becomes possible.

– Standing up a test environment with up-to-date can be added to the CI/CD rig.

– Faster development cycles which translate in faster go to market features.

– All automated by code

Hewlett Packard
Enterprise
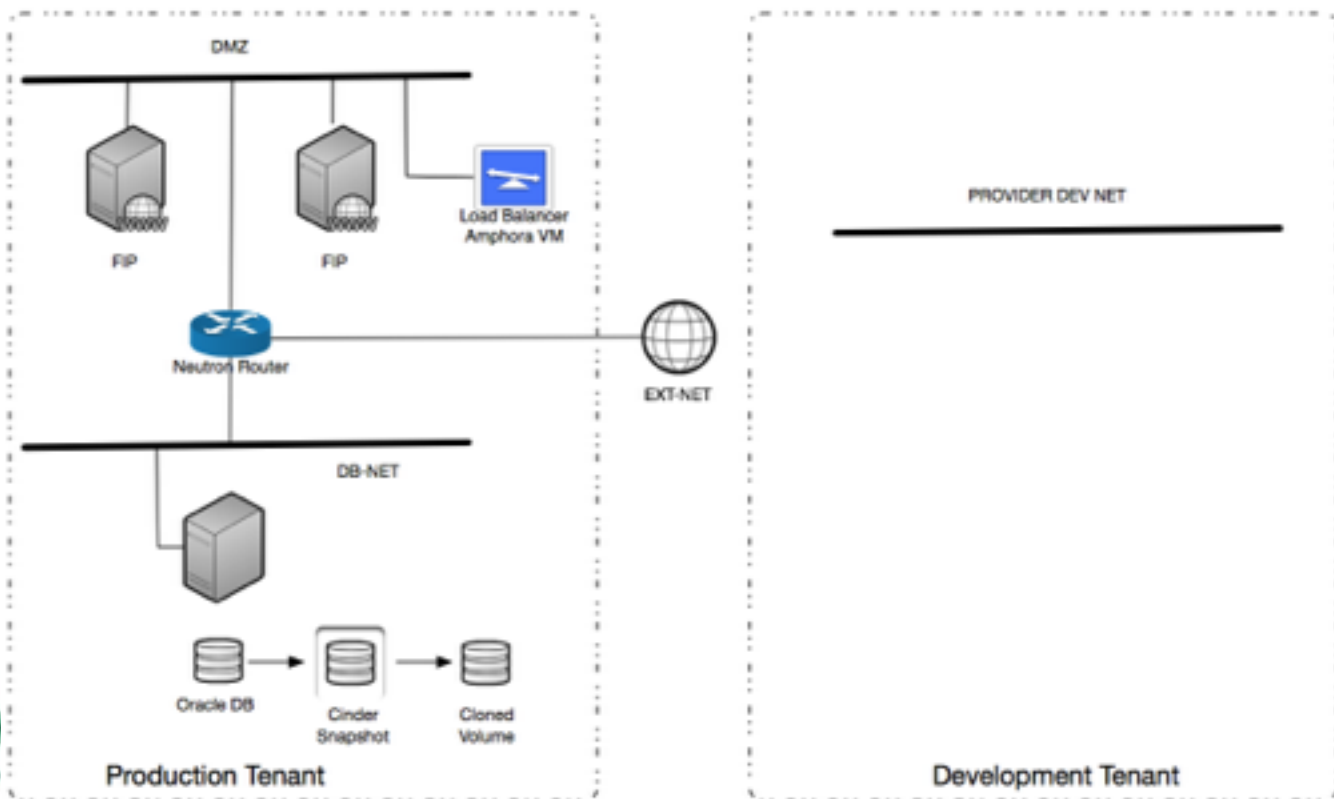
Data Cloning as a Service Demo

Stage 1:

Stage 2:

Stage 3:

DMZ

FIP   FIP   Load Balancer
                          Amphora VM

Neutron Router

EXT-NET

DB-NET

Oracle DB → Snapshot Removed → Cloned Volume Transferred

PROVIDER DEV NET

Production Tenant   Development Tenant

Hewlett Packard
Enterprise

19
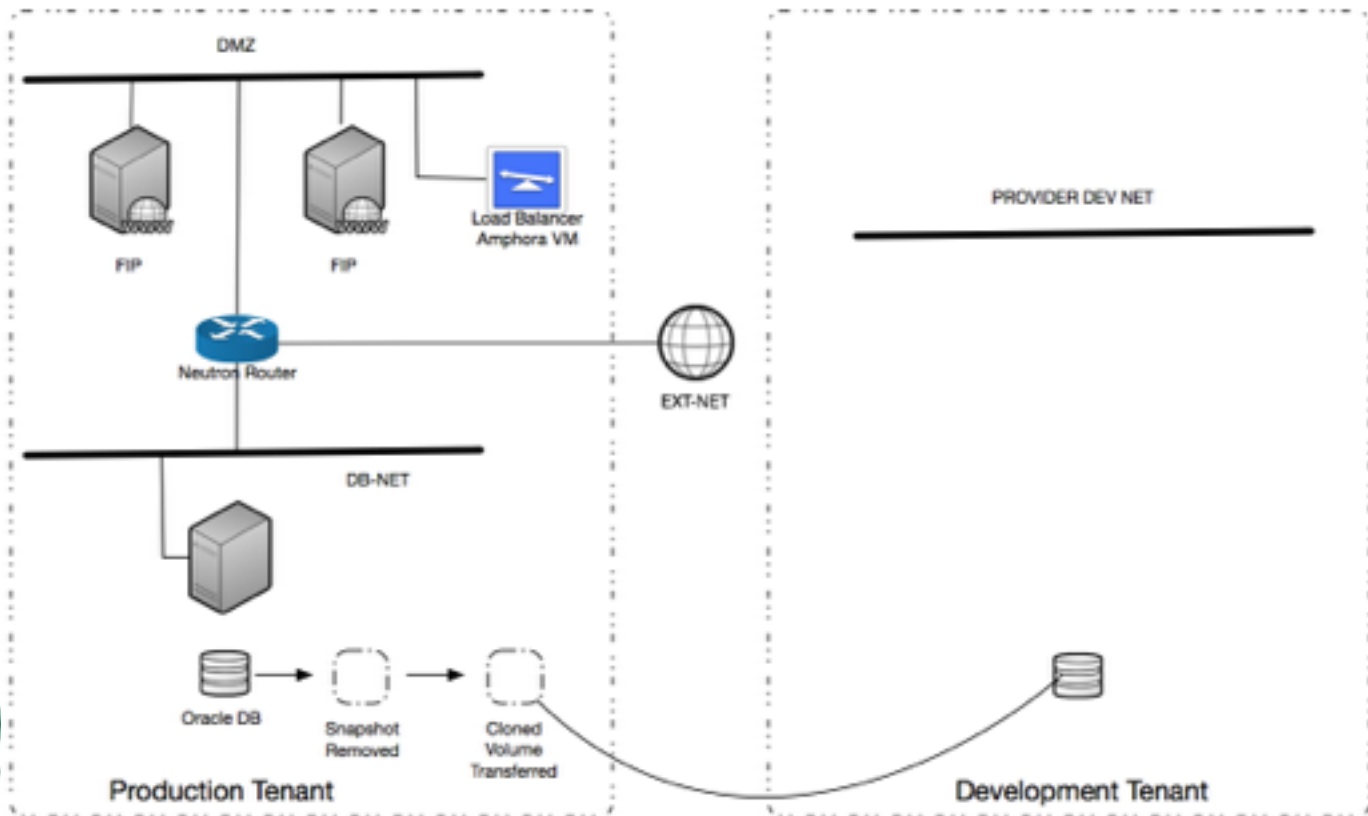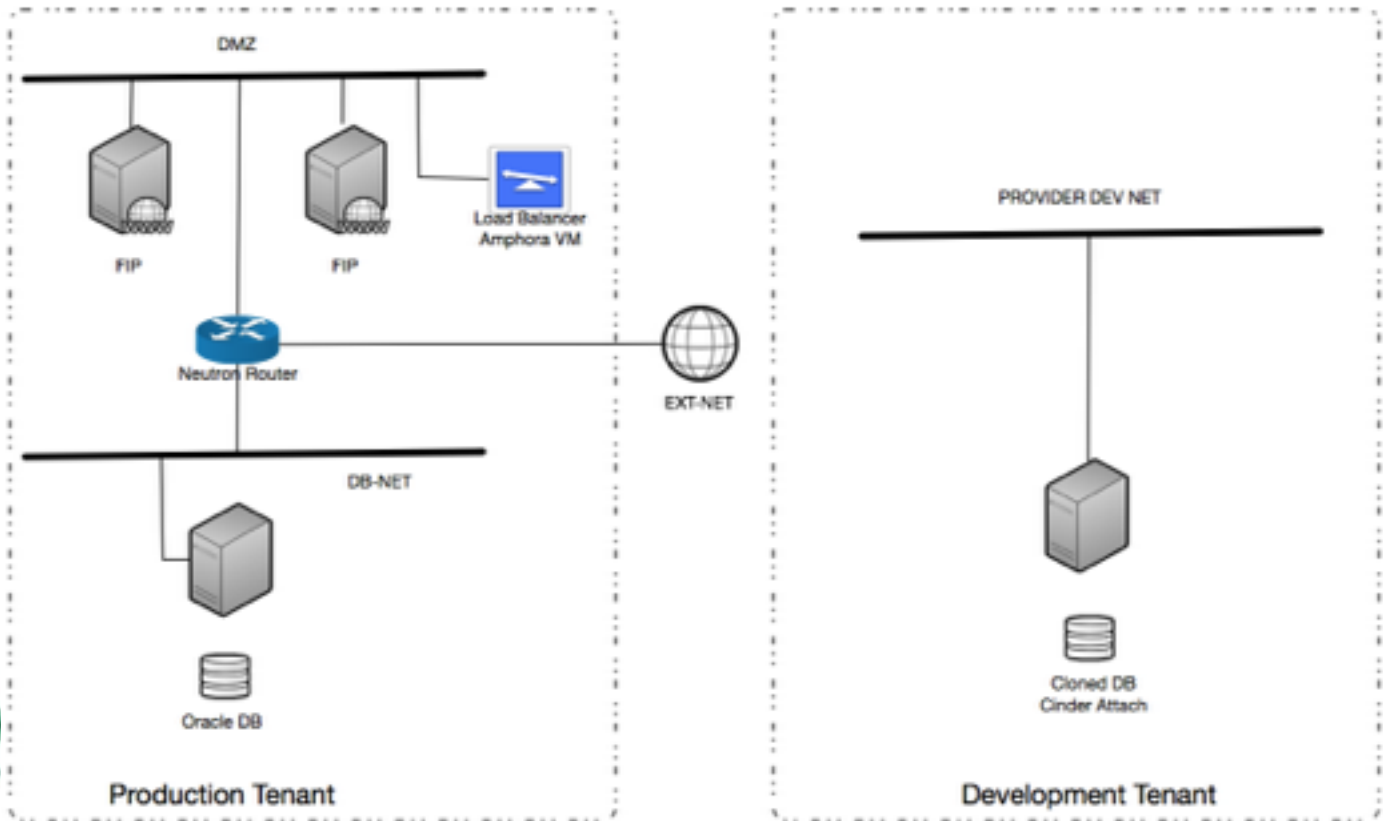
Stage 4:

Thank you

Github repo:

GitHub, Inc. [US] | https://github.com/gatesch/ansible/
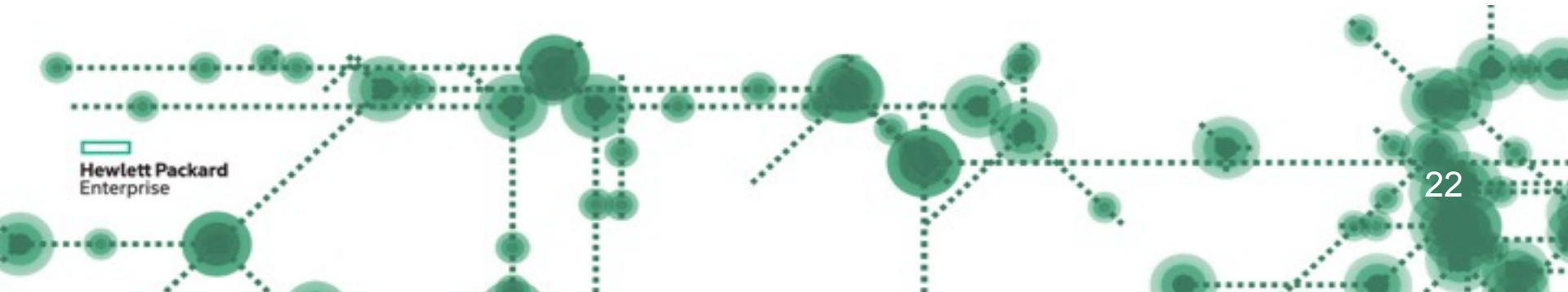
Personal Open source Business Explore   Pricing Blog Support   This repository Search   Sign in   Sign up

gatesch / ansible   Watch 1   ★ Star 0   Fork 0

<> Code   ⊙ Issues 0   Pull requests 0   Projects 0   Pulse   Graphs

Ansible Playbooks for OpenStack

Hewlett Packard
Enterprise