PayPal’s Private Cloud @ Scale

Jigar Desai • @jigardesai • March 17 2016
<table>
<thead>
<tr>
<th>Table of contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to PayPal</td>
</tr>
<tr>
<td>Current Cloud Stack</td>
</tr>
<tr>
<td>SDN Journey</td>
</tr>
<tr>
<td>Future Cloud Stack</td>
</tr>
<tr>
<td>Q&amp;A</td>
</tr>
</tbody>
</table>
Introduction to PayPal

A Technology Perspective
About PayPal

PayPal is a leading technology platform company that enables digital and mobile payments on behalf of consumers and merchants worldwide. We put our customers at the center of everything we do. We strive to increase our relevance for consumers, merchants, friends and family to access and move their money anywhere in the world, anytime, on any platform and through any device.
Architecture @ PayPal
Robust Infrastructure, Reusable Platforms, Payments Operating System, Delightful Experiences
Cloud@PayPal
Key Statistics

Developer Statistics

- x 1000 engineers
- x 10M Lines
- x 1000 Releases/year
- x 1000 Builds/day
- x 1000 Deploy/day

OpenStack Cloud

- 3 Regions
- 9 Availability Zones
- x 100K Cores
- > 10K Physical Servers
- x 10K VMs
- x 10 PB Storage
- > 1000 Services
Impact On Life Of A Developer

2 years back

- QA Deployment: 8 Weeks
- Build Time: 2.5 Hours
- Prod Deployment: 4 Hours
- Infrastructure: 1 Month

Now

- QA Deployment: 1 Day
- Build Time: 5 Minutes
- Prod Deployment: < 30 Minutes
- Infrastructure: 30 Minutes

© 2015 PayPal Inc. All rights reserved. Confidential and proprietary.
The Current Cloud Stack

- Datacenters (Geographic regions, Availability Zones)
- OpenStack Cloud (Infrastructure as a Service)
- Platform as a Service
- Web/Mid Tier Applications

Common Infrastructure

- 100% of web and mid tier applications on OpenStack
- Proprietary PaaS on top of OpenStack to automate E2E application development lifecycle
- Support for polyglot applications
- Test and production environments available on-demand

Common Platforms and Services

- Java
- Node
- Scala
Cloud SDN Journey
Why SDN at PayPal?

• Ability to logically isolate cloud resources (compute, storage, network) for different business use cases needing different security policies while co-existing on shared infrastructure
• Solve compute capacity islands by moving computes between security zones as needed
• Programmatic APIs to enable both cloud users and operator reducing operational overhead
• Use cases:
  • External zone hosting beta apps reachable from internet but separated from other zones
  • Developer zone hosting all developer tools with no direct access from internet but available from corp
Our SDN Architecture

PayPal deploys multiple VPCs (Virtual Private Clouds) in every AZ
Every overlay VPC is running on a separate routed network and firewalled off
Bridged VPCs are deployed using VRF (Virtual Routing and Forwarding)
SDN controllers are horizontally scaled
SDN Challenges

- Off the shelf solutions are not battle-tested for scale well
  - Example: Control plane doesn’t scale well beyond 2500 hypervisors
- Bit early in software maturity curve
  - Example: Latency issues with early OVS implementation
  - Security groups performance issues with multiple rules. Later solved with “megaflows” feature
- Strong architectural principles don’t always mean strong implementation
  - Initial SDN implementation didn’t have full separation between control plane and data plane. Control plane outages resulted in site outages
- Security concerns specially around centralized control plane
The Future
The Future Cloud Stack

- Datacenters (Geographic regions, Availability Zones)
- OpenStack Cloud (Infrastructure as a Service)
- Web and Mid Tier Applications
- Public Clouds

- Common Infrastructure
- Common Platforms and Services

- New PaaS is being built using Mesos and Docker on top of OpenStack
- Goal is to achieve industry leading datacenter efficiency and utilization
- High application resiliency against infrastructure failures
- Hybrid cloud POC
- PaaS support for stateful applications
Container Networking
Container Networking Needs

Needs:
• Containers as first class citizens of the network
• IP per container or per pod
  • Container IP must be a private address routable within the AZ
• Low latency container to container communication
• Support up to 100 containers per host
• Distributed SLB
• IP Mobility within the AZ for stateful apps
• Distributed firewall

Exploratory Options:
Non-overlay: Ipvlan, Macvlan
Overlay: Vxlan, MPLS
Questions?
Jdesai at paypal dot com