Pivotal CF

Technical Overview

September 2014

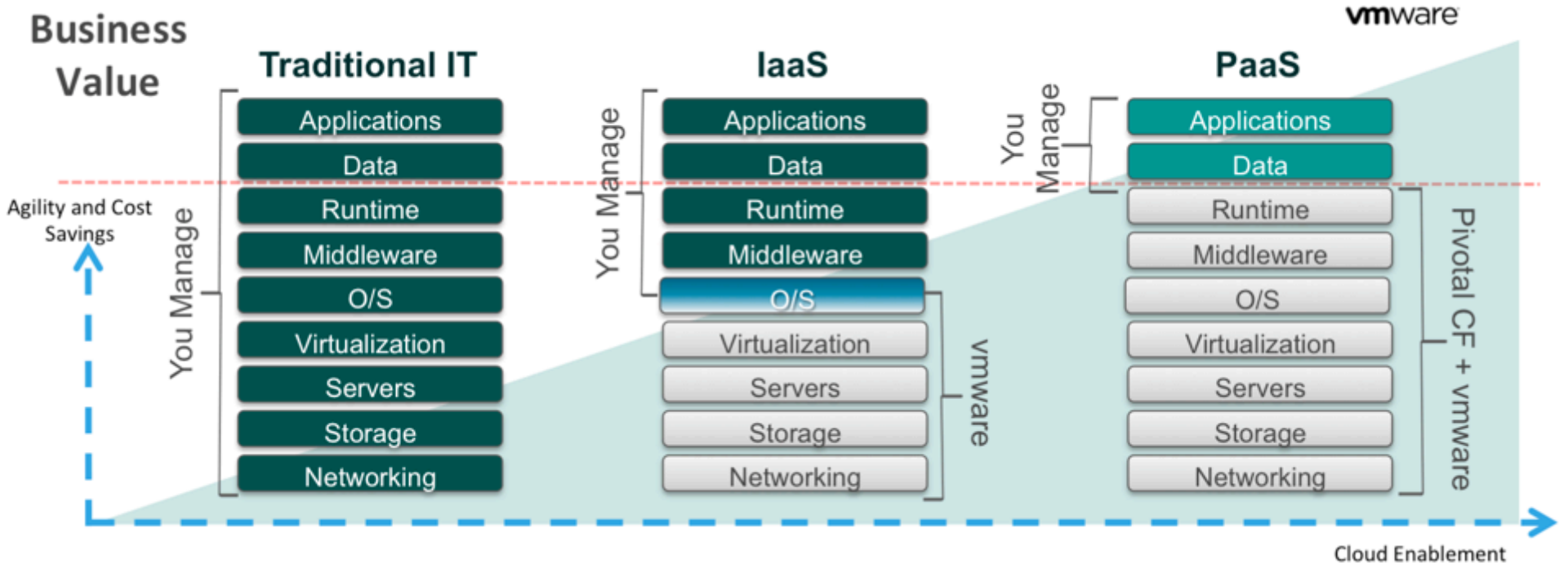
Pivotal

Outline

- Overview and Architecture
- Deployment - Applications and Services
- Health Management – Applications and Platform
- Isolation – Networks, Containers, Org, Spaces
- Security – Access Control, Security Groups and Identity
- Operational Manager - Behind the Scenes

Pivotal

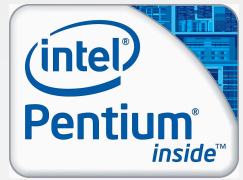
The Cloud Platform Evolution



Pivotal

The world is spinning faster

1999

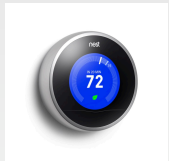


Decades

200X

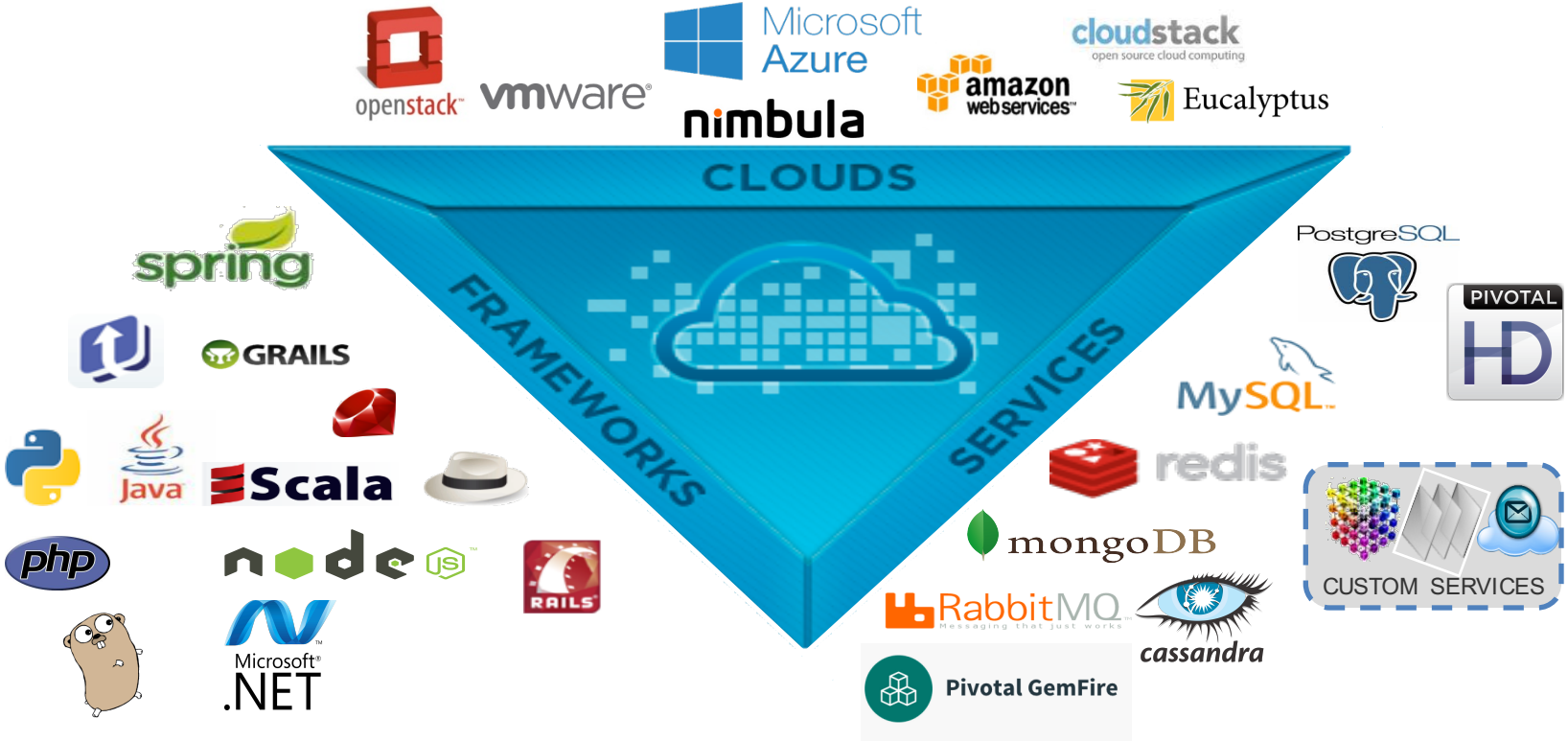
Years

201X



????

The Open Platform as a Service



Pivotal

Pivotal CF Enterprise PaaS

Automatic AppServer & OS Configuration with Buildpacks *("just push your app")*

Application Containerization & Cluster Scheduling

Application Network Security Groups

Application to Services Binding and Access

App Health Mng, Load Balancing, Rapid Scaling, Availability Zones

Policy, Identity and Roles Management

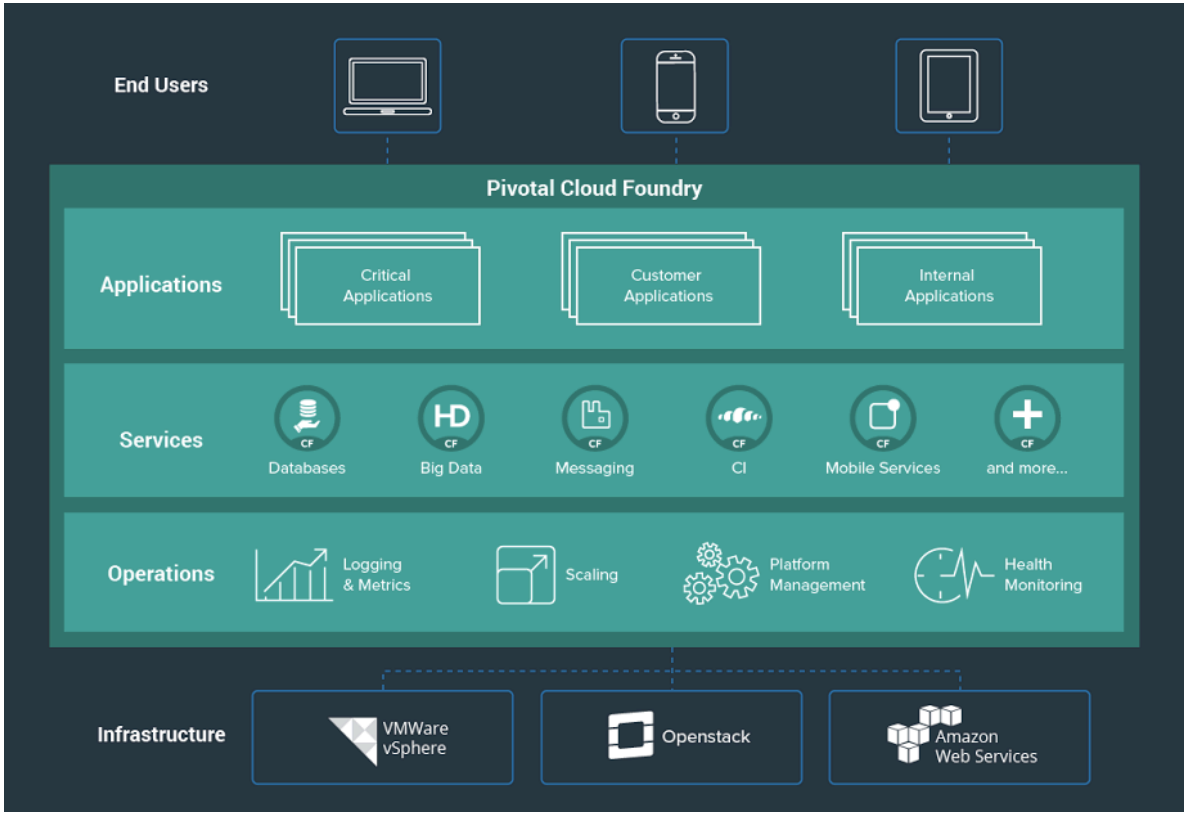
Native & Extended Data, Mobile and Platform Services

IaaS Provisioning, Scaling & Configuration

Logging as a service, Application metrics & performance, Metric based scaling

Pivotal

Pivotal Cloud Foundry Integrated Platform



Developers Agility:

$ target <my environment>

$ push <my app>

$ bind <service instance>

$ scale <my app> +1000

Operational Agility:

$ provision cloud <public/private>

$ provision service <service tile>

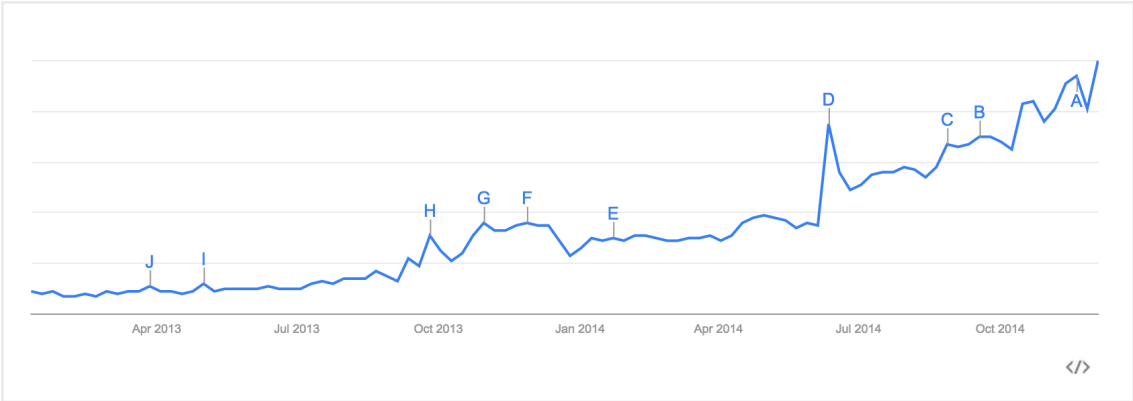
$ upgrade/update <my cloud>

$ scale <my cloud>

Pivotal

Containers

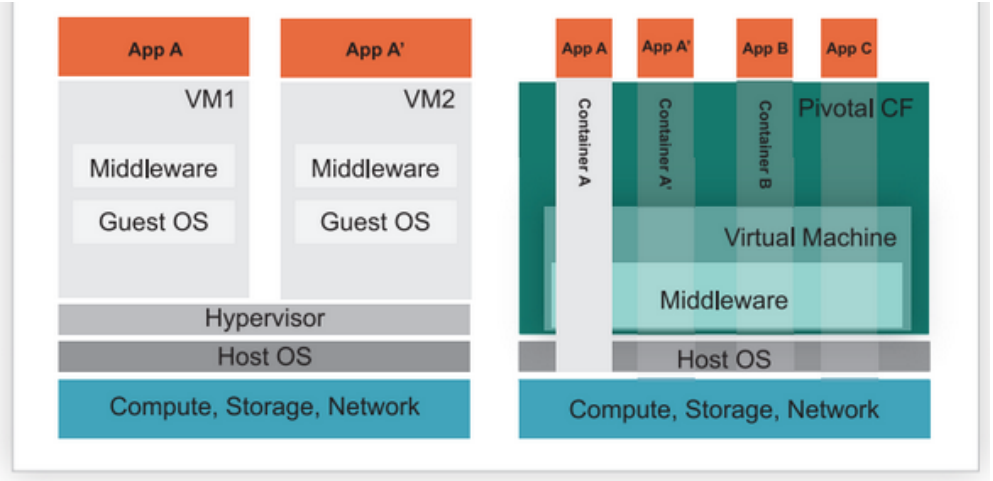
- In Dec 2013 docker was on no one's radar
- In Dec 2014 docker is on everybody's radar



Pivotal

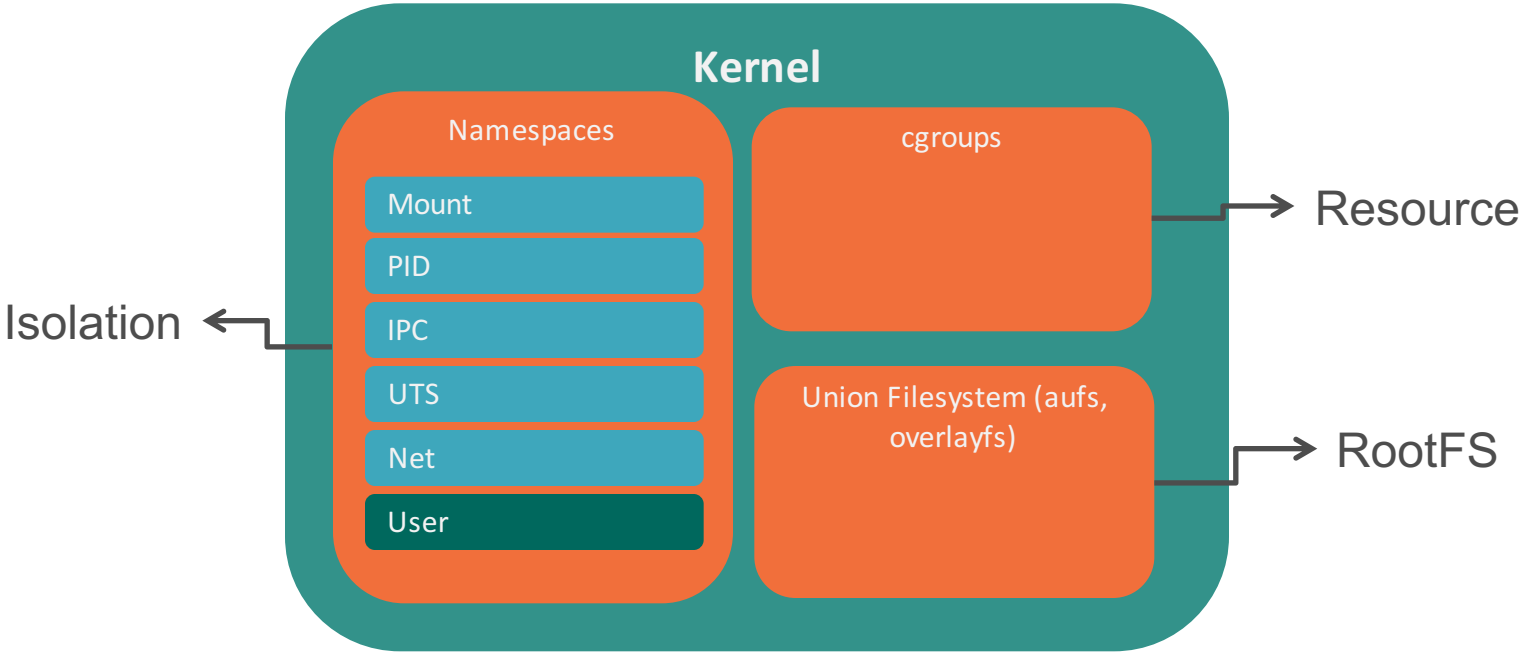
Containers

- Increased server utilization, portability, consistency and speed
- Reduced OS footprint
- Multiple application instances per VM means higher workload density



Pivotal

Containers



Containers Alone Aren't Enough…

- Orchestration & Management of Application Instances
  - Apps span multiple containers and VMs
  - Automated responses mitigate failure conditions
  - Load balancing and performance tuning
  - Instant scaling to support workloads
- Application-centric Security
  - Role-based access control
  - Logging and event auditing
  - App

Pivotal

Containers are not enough

- Containers date back to 2008 (LXC)
- cgroups contributed back from google
- Docker created in 2013
- Much like compute and VMs, containers alone are commodities

Pivotal

It takes a platform…

Pivotal CF

Spring Cloud

Pivotal

Automatic Configuration with Buildpacks

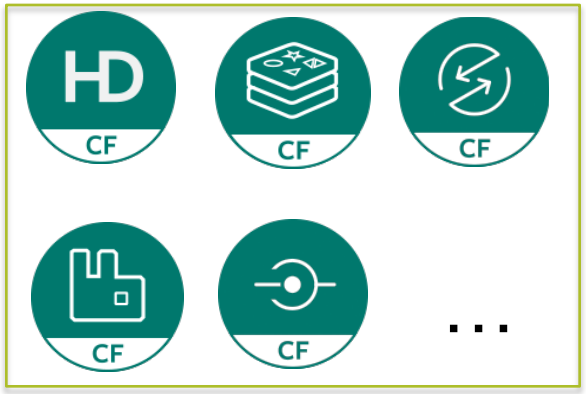
Provide developers wide choice, multi-lingual runtime support, all in a single platform

- PCF automatically detects and installs buildpack, so your app is ready to run
- Growing list of supported Frameworks, Tools & Languages
- Support polyglot platform. Reduce complexity for developers and costs to manage multiple frameworks

Pivotal

Pivotal Cloud Foundry Services

Access to a large (growing) ecosystem of Services, integrated and managed, user-provided, and custom – true self-provisioning for developers and IT operators.



Pivotal Technologies

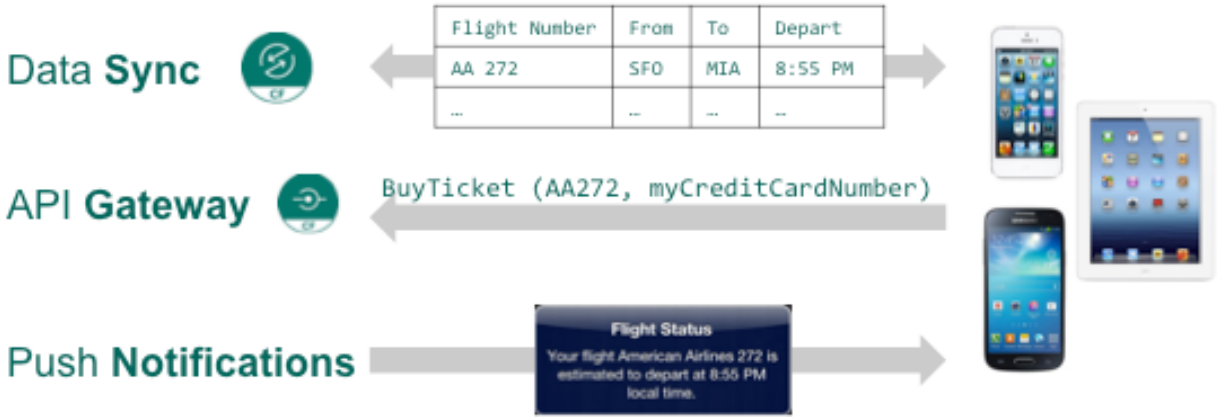
Partner Services

Custom Services

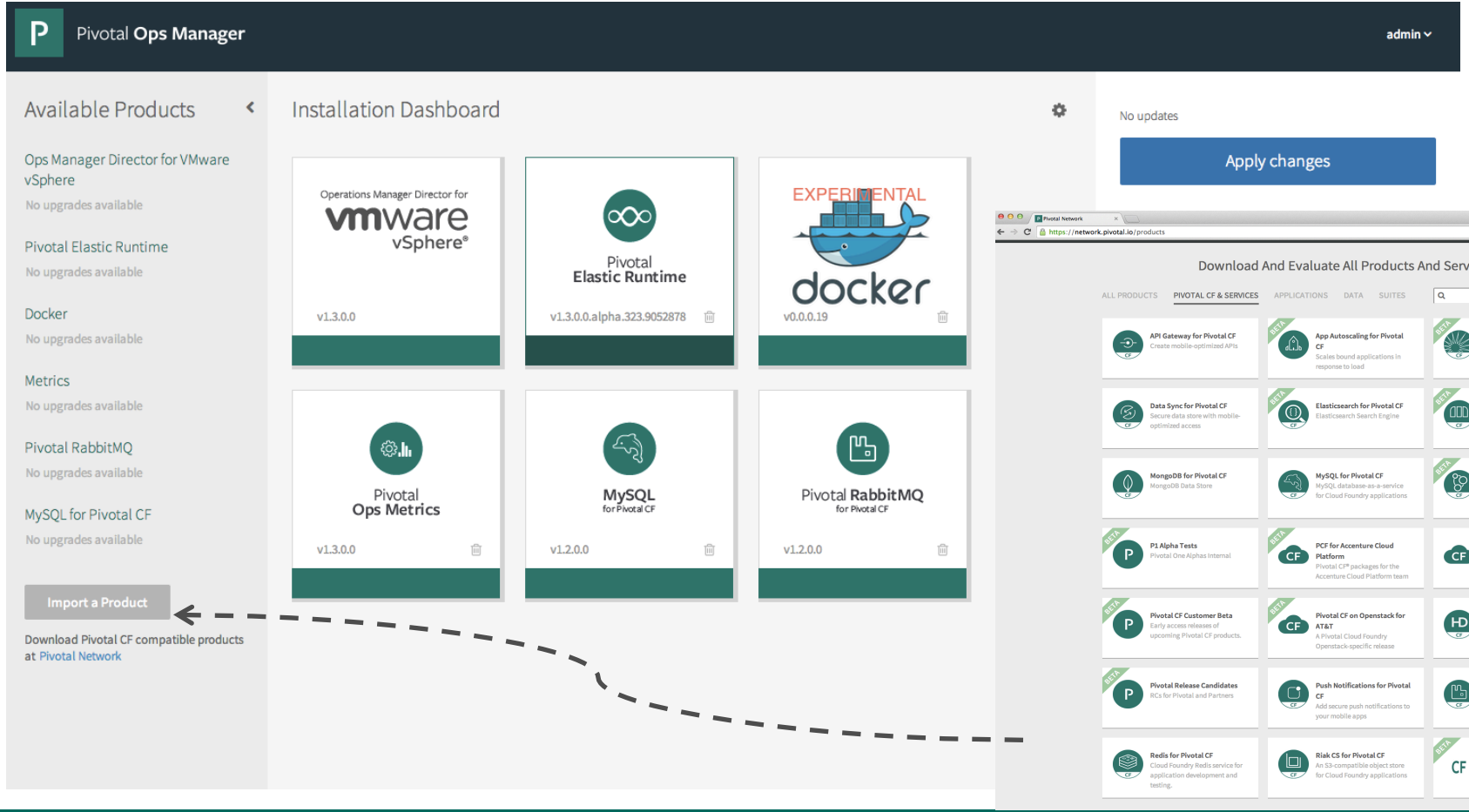
Pivotal Cloud Foundry Mobile Services
Rapid Mobile Apps

Build Mobile Apps Faster

- *Data sync* between data sources & mobile apps
- *Remote API calls* from mobile apps
- *Push notifications* to mobile apps



Pivotal

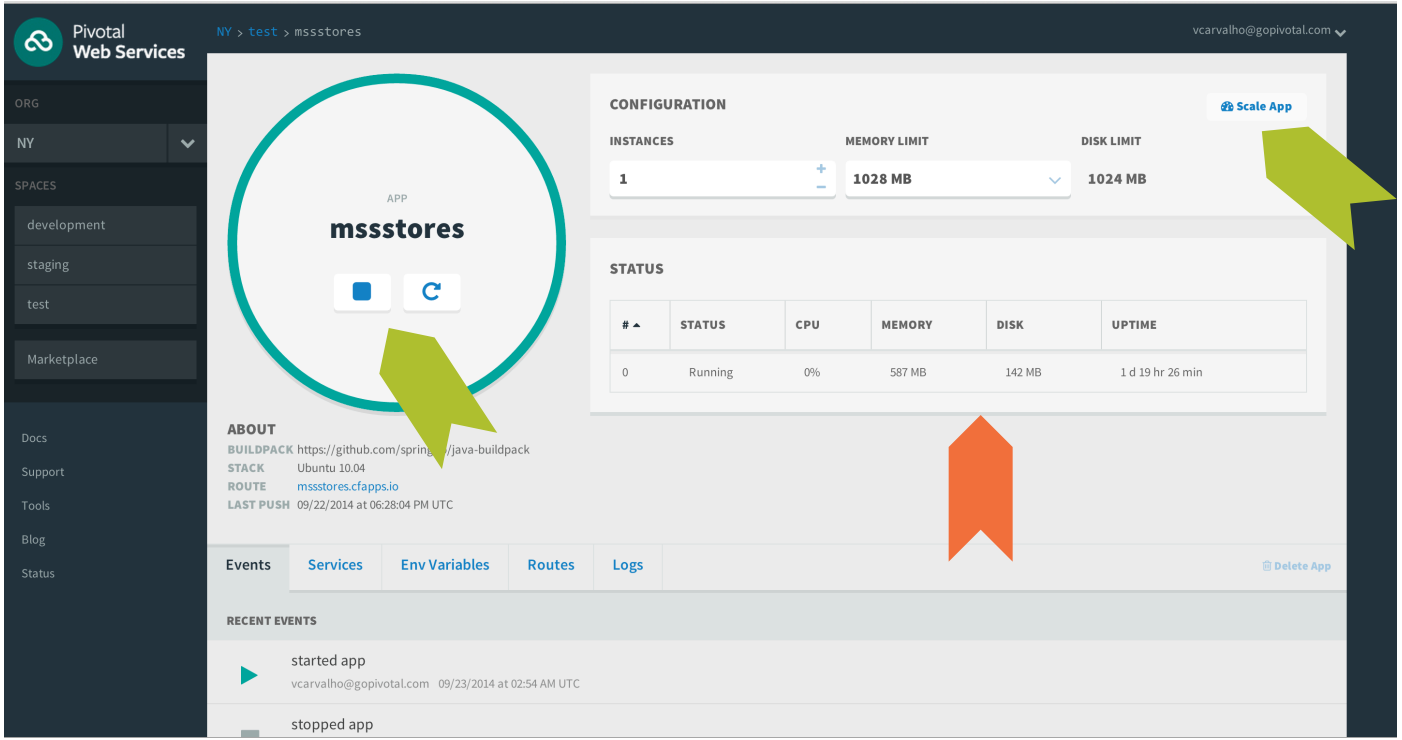


Pivotal

Rapid Provisioning

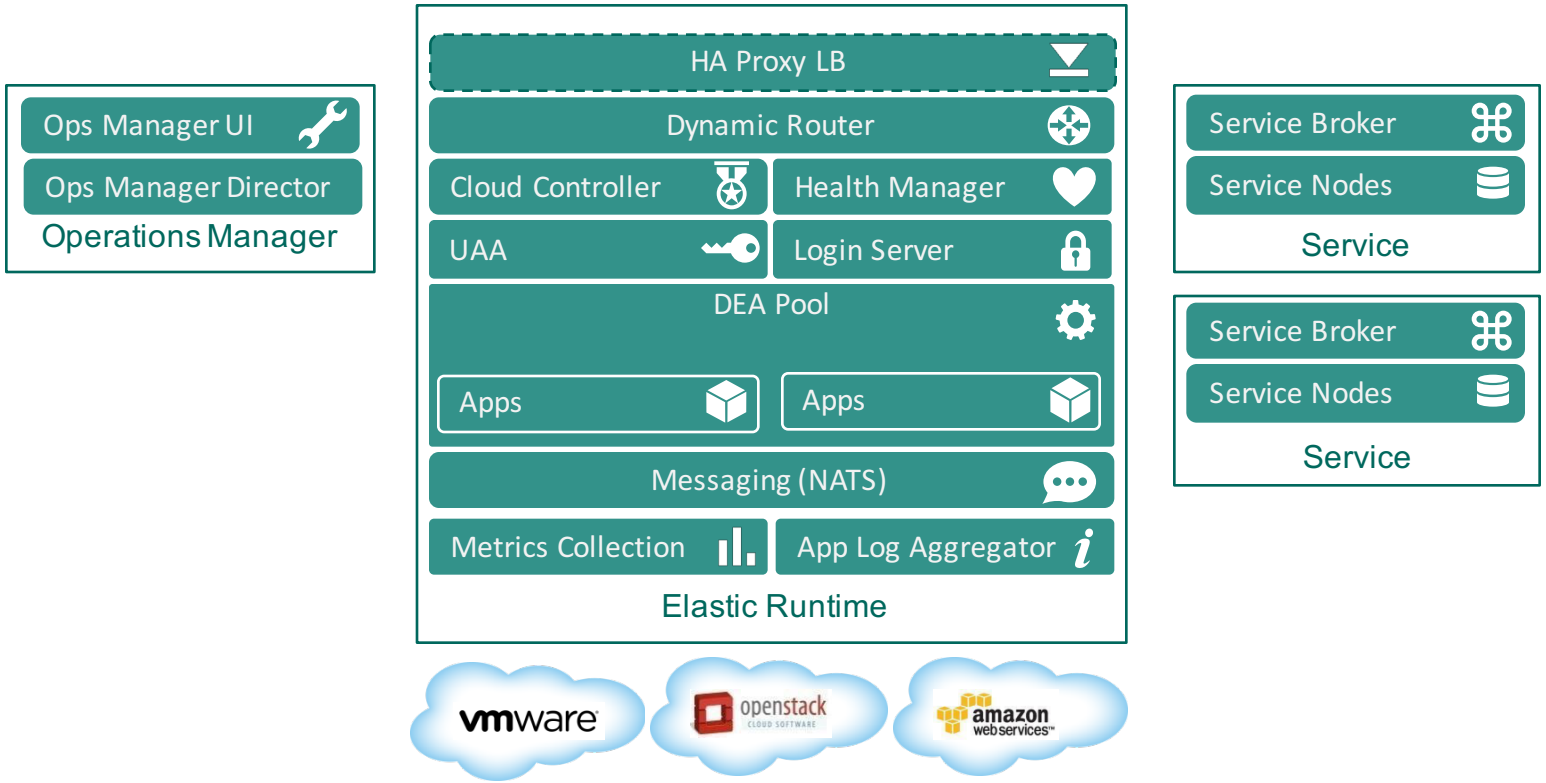
Monitoring

Rapid Application deployment



Pivotal

Pivotal CF Architecture



Pivotal

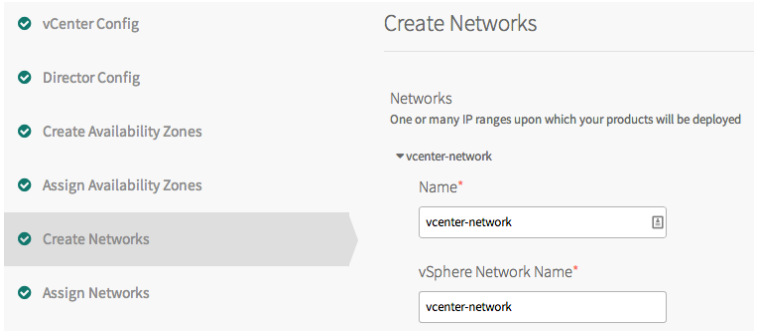
Isolation

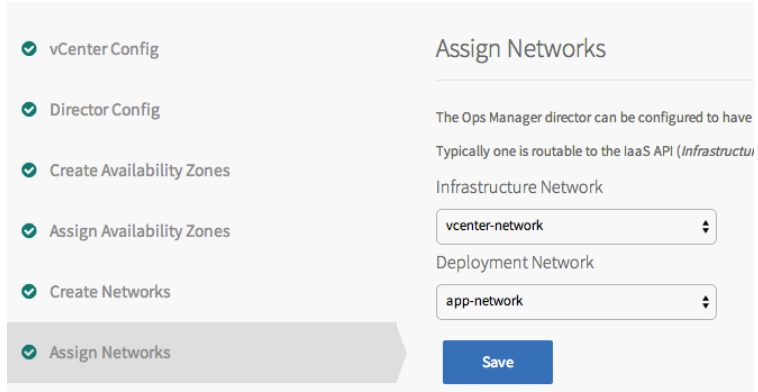
Networks, Containers, Org, Spaces

Pivotal

Multiple Networks to Safeguard Infrastructure

- Operator selects IaaS network for each product deployment
  - Provides isolation
  - Network layout flexibility



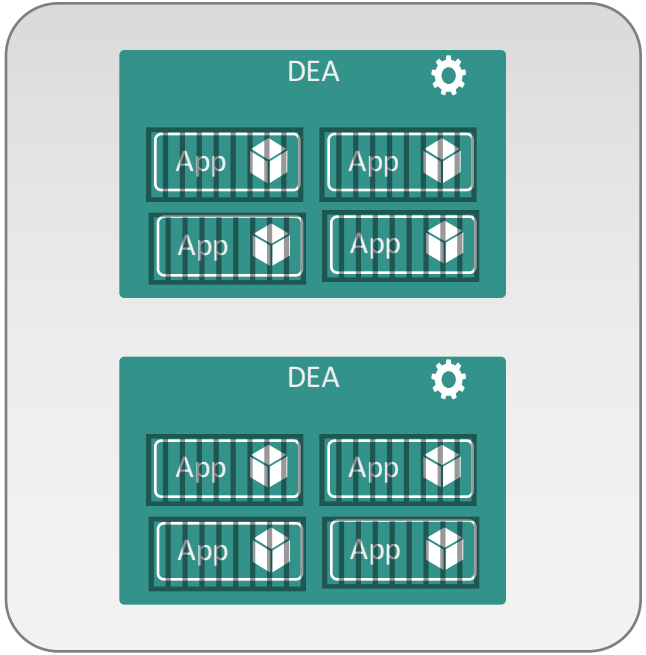


Pivotal

Container Isolation

Containers provide isolation of resources – CPU, memory, file system, process space, network

Containers have their own private network, not accessible from outside the DEA

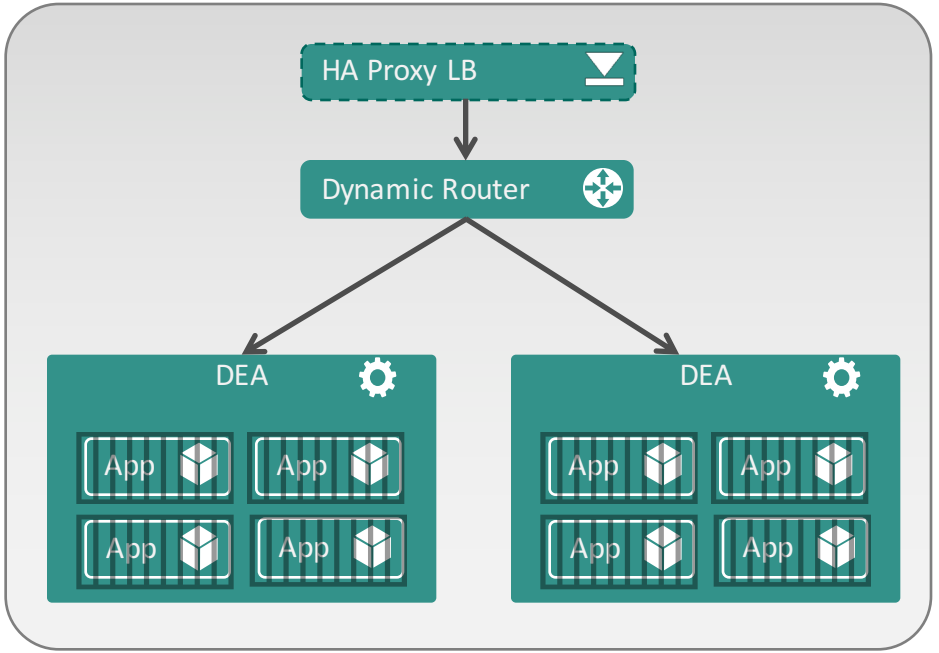


Pivotal

Container Isolation

Routers forward requests from outside using the app's route to the assigned port on the DEA, which does network translation to the container's internal IP and port

Apps are prevented from communicating directly with each other by container firewall rules; they must communicate through published routes



Pivotal

Organizations

Logical divisions for tenants, having their own Quotas and Users

User permissions are specified per Org and Space

User administration is delegated to the Org level

ORGANIZATION ROLES

ORGANIZATION MANAGER
Can invite/manage users, select/change the plan, establish spending limits

ORGANIZATION AUDITOR
Read-only access to org info and reports

Pivotal

Spaces

Logical sub-division inside an Org

Users specified at the Org level can have different access levels per Space

Services and Applications are scoped to a Space

Optional Quotas at the Space level

APP SPACE ROLES

SPACE MANAGER
Can invite/manage users, enable features for a given space

SPACE DEVELOPER
Can create, delete, manage applications and services, full access to all usage reports and logs

SPACE AUDITOR
Read-only access to all space information, settings, reports, logs

Pivotal

Deployment

Applications and Services

Pivotal

Deployment styles

IaaS (simplified)

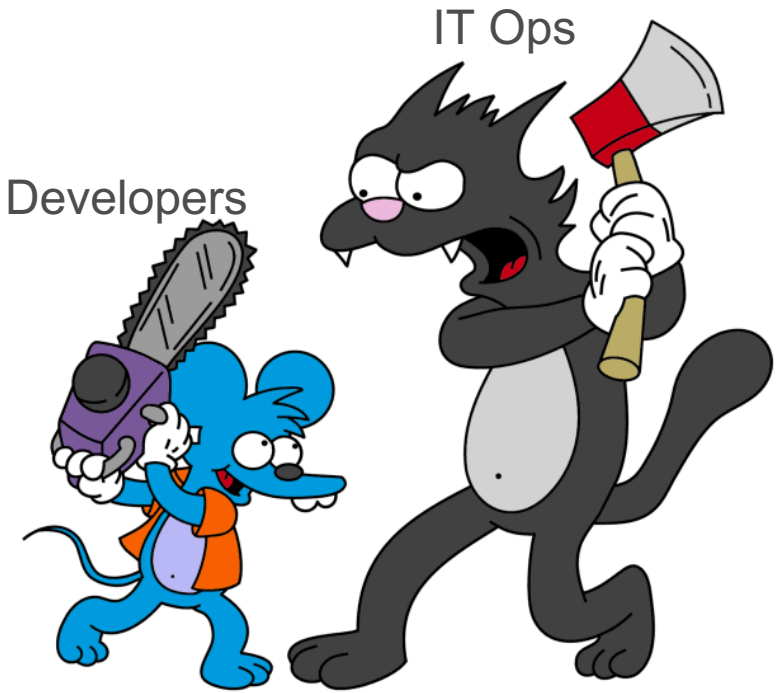
```
gcutil --project=<project-id> adddisk <disk-name> [--size_gb=<size> --zone=<zone-name> \
       --source_snapshot=<snapshot-name> --source_image=<image-name>] --disk_type=<disk-type>
gcutil --project=myproject addfirewall icmpfirewall --allowed=icmp
gcutil addfirewall http2 --description="Incoming http allowed." --allowed="tcp:http"
gcutil --project=<project-id> reserveaddress --region=<region> [--source_address=<ephemeral-address>] <address-name>
gcutil  --project=<project-id> addinstance --external_ip_address=<external-ip> --machine_type=<machine-type>
--image=<fully-qualified-image-name> --disk=<disk-name>[,deviceName=<alias-name>,mode=<mode>,boot] --[no]auto_delete_boot_disk
--boot_disk_type=<disk-type> --service_account_scope=<scopes>
gcutil addinstance --authorized_ssh_keys=username1:/path/to/keyfile1,username2:/path/to/keyfile2,...
gcutil ssh <instance_name>


apt-get install openjdk7
mkdir /usr/local/tomcat
wget http://apache.mesi.com.ar/tomcat/tomcat-7/v7.0.54/bin/apache-tomcat-7.0.54.zip
unzip apache-tomcat-7.0.54.zip
vim /conf/server.xml
vim /etc/init.d/tomcat
chmod a+x /etc/init.d/tomcat
update-rc.d tomcat defaults
service tomcat start

scp myapp.war root@machine:/usr/local/tomcat/webapps
```

CF (verbose mode)

```
cf push myapp
```

Pivotal

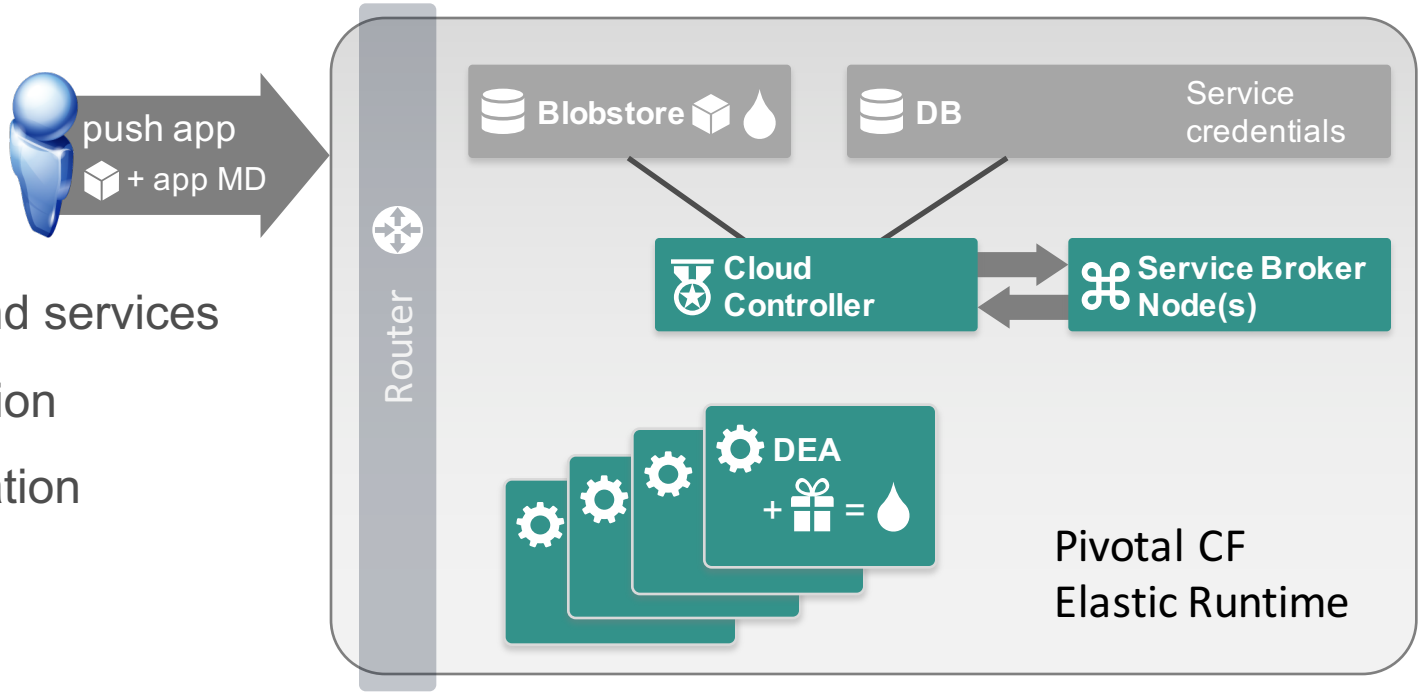
Demo #1 : Pushing an application



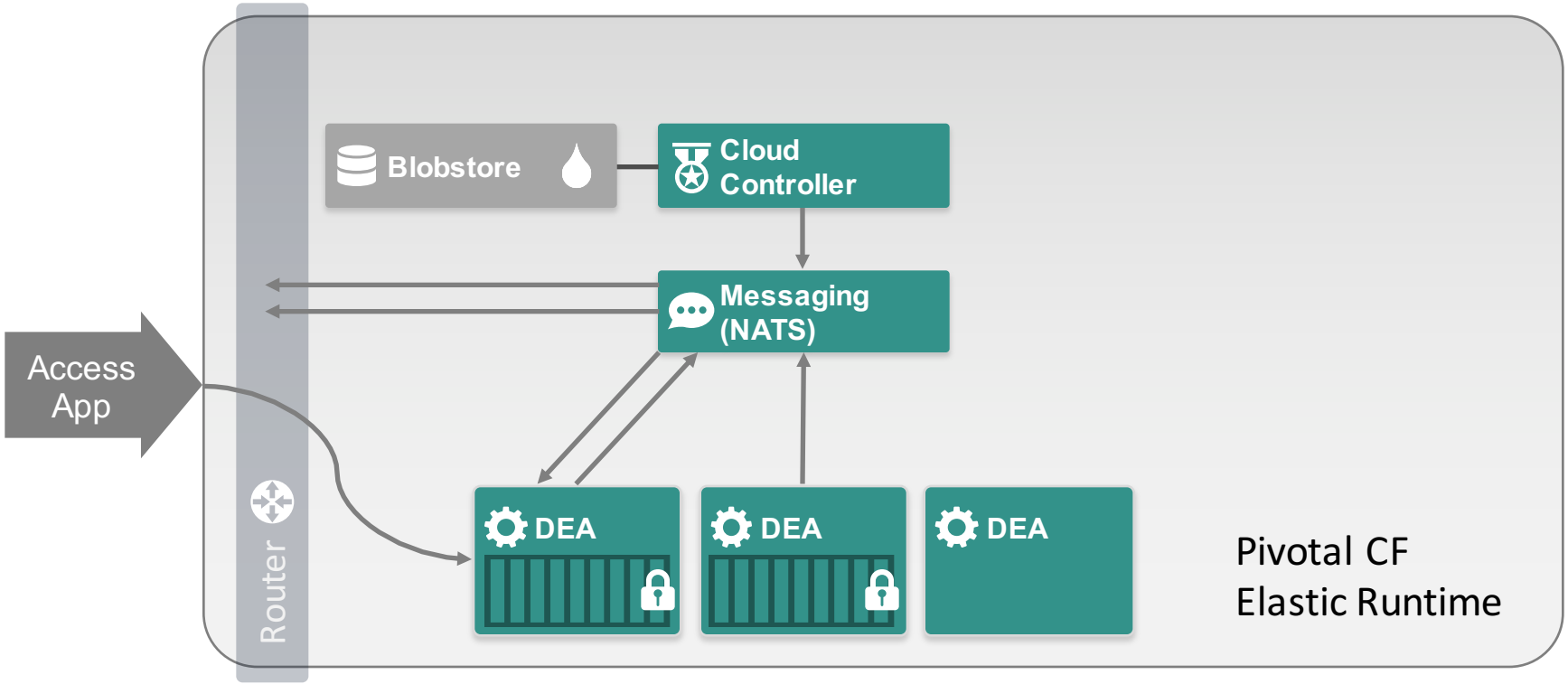
Pivotal

Application Deployment Overview

1. Upload app bits and metadata
2. Create and bind services
3. Stage application
4. Deploy application

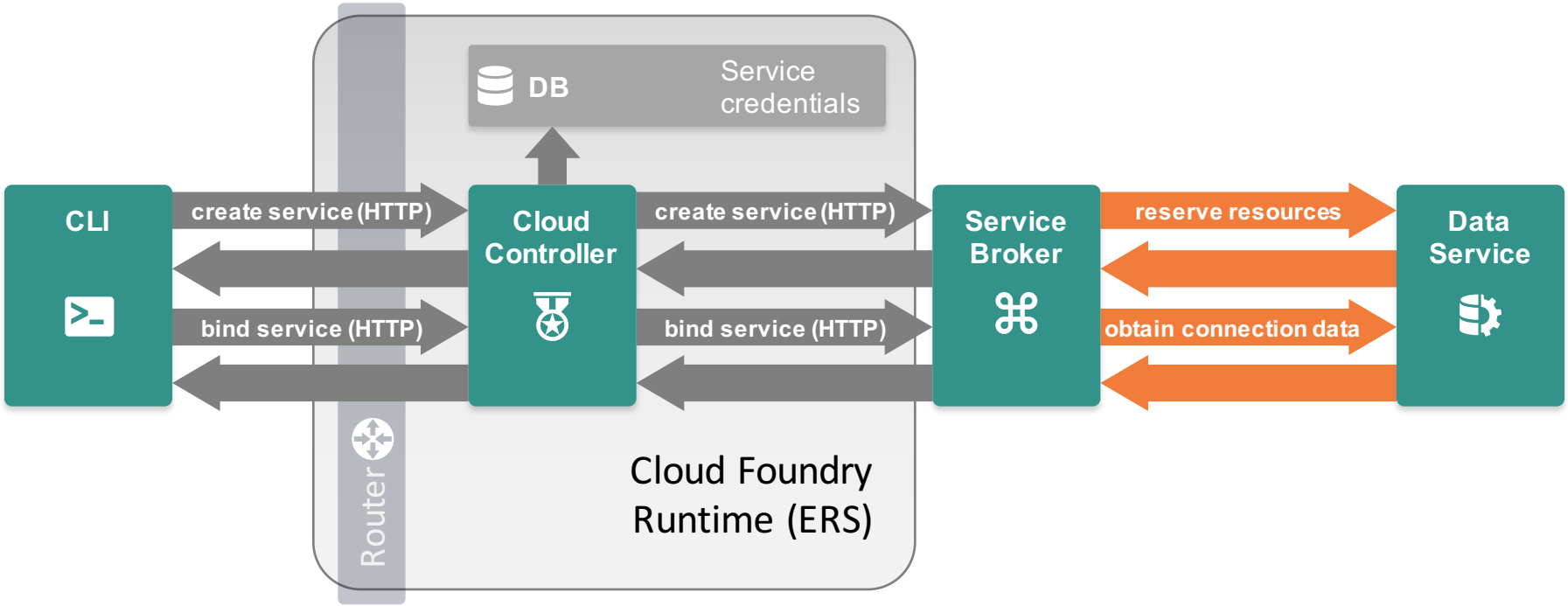


Deploying an *Application*



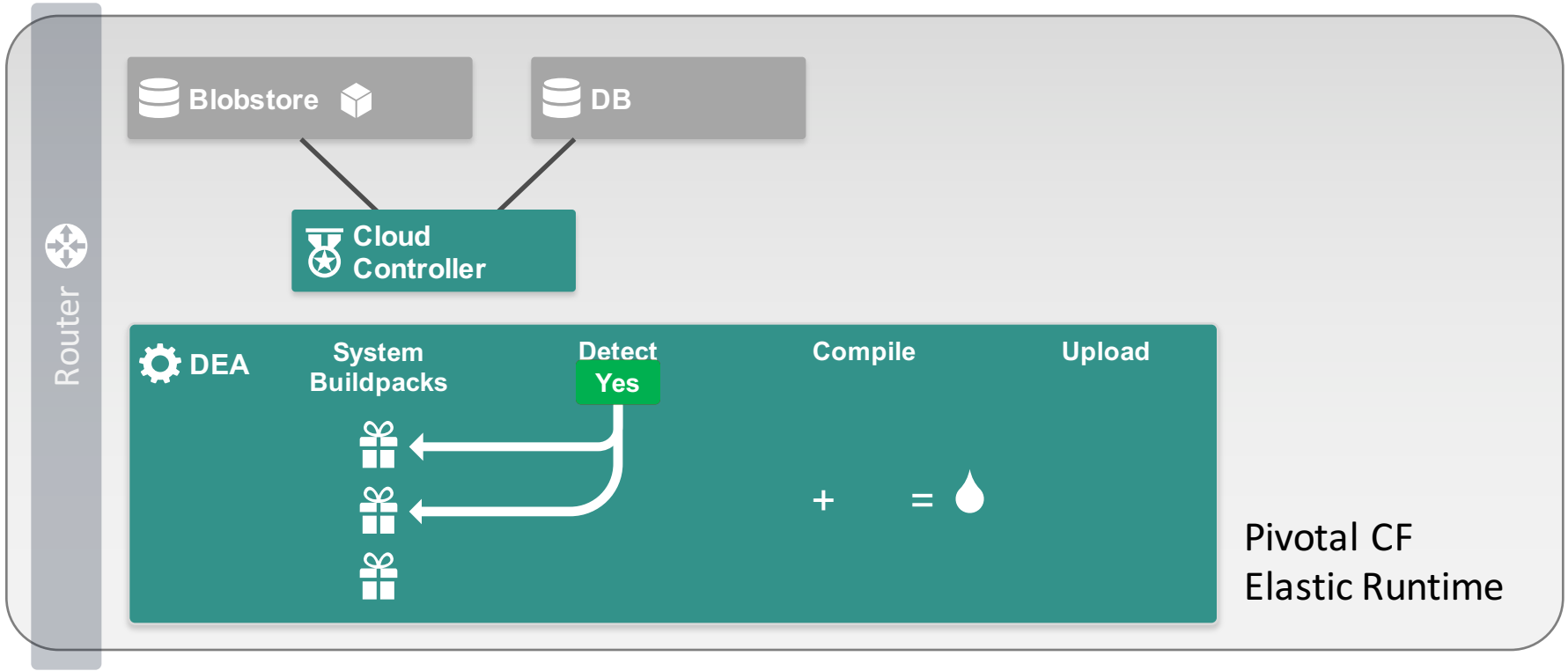
Pivotal

Creating and Binding a *Service*



Pivotal

Stage an *Application*

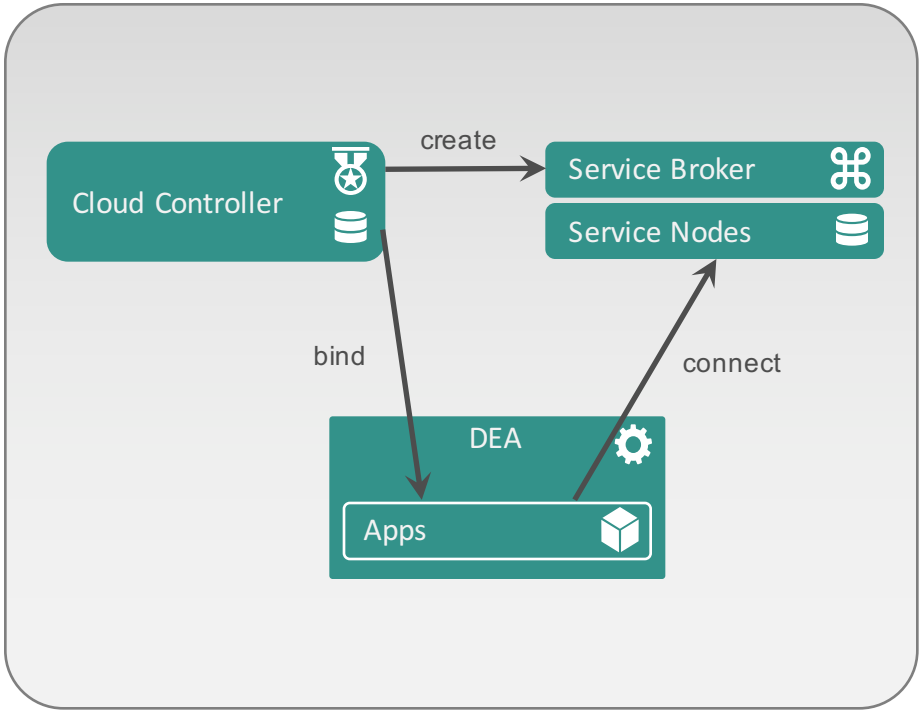


Managed Services

Service Brokers generate connection details and credentials for managed services

CC encrypts and stores credentials in CCDB

Credentials are exposed to bound applications via VCAP_SERVICES environment variable



Pivotal

Managed Services

VCAP_SERVICES environment variable is visible only to members of the org and space containing the service instance

```
VCAP_SERVICES=" {
 "p-mysql": [
  {
   "name": "music-db",
   "label": "p-mysql",
   "tags": [ "mysql", "relational" ],
   "plan": "100mb-dev",
   "credentials": {
    "hostname": "192.168.1.147",
    "port": 3306,
    "name": "cf_aceae021_7f27_48db_9844_d7c151f29195",
    "username": "Tr12ZI4hPu4OPJPY",
    "password": "fuTWBqpGeyvv0qge",
    "uri": "mysql://Tr12ZI4hPu4OPJPY:fuTWBqpGeyvv0qge@192.168.1.147:3306/
                cf_aceae021_7f27_48db_9844_d7c151f29195?reconnect=true"
   }
  }
 ]
} "
```

Pivotal

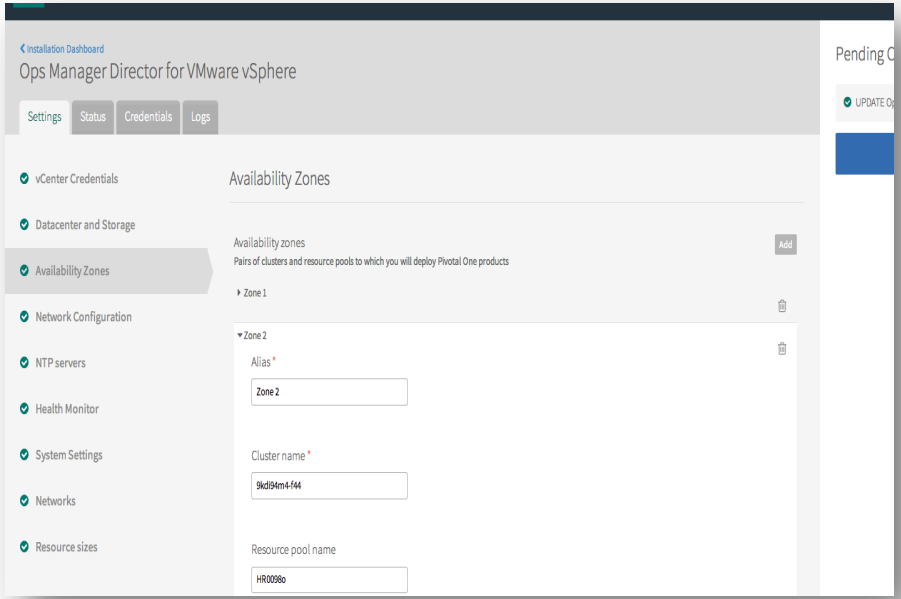
Health Management

Applications and Platform

Pivotal

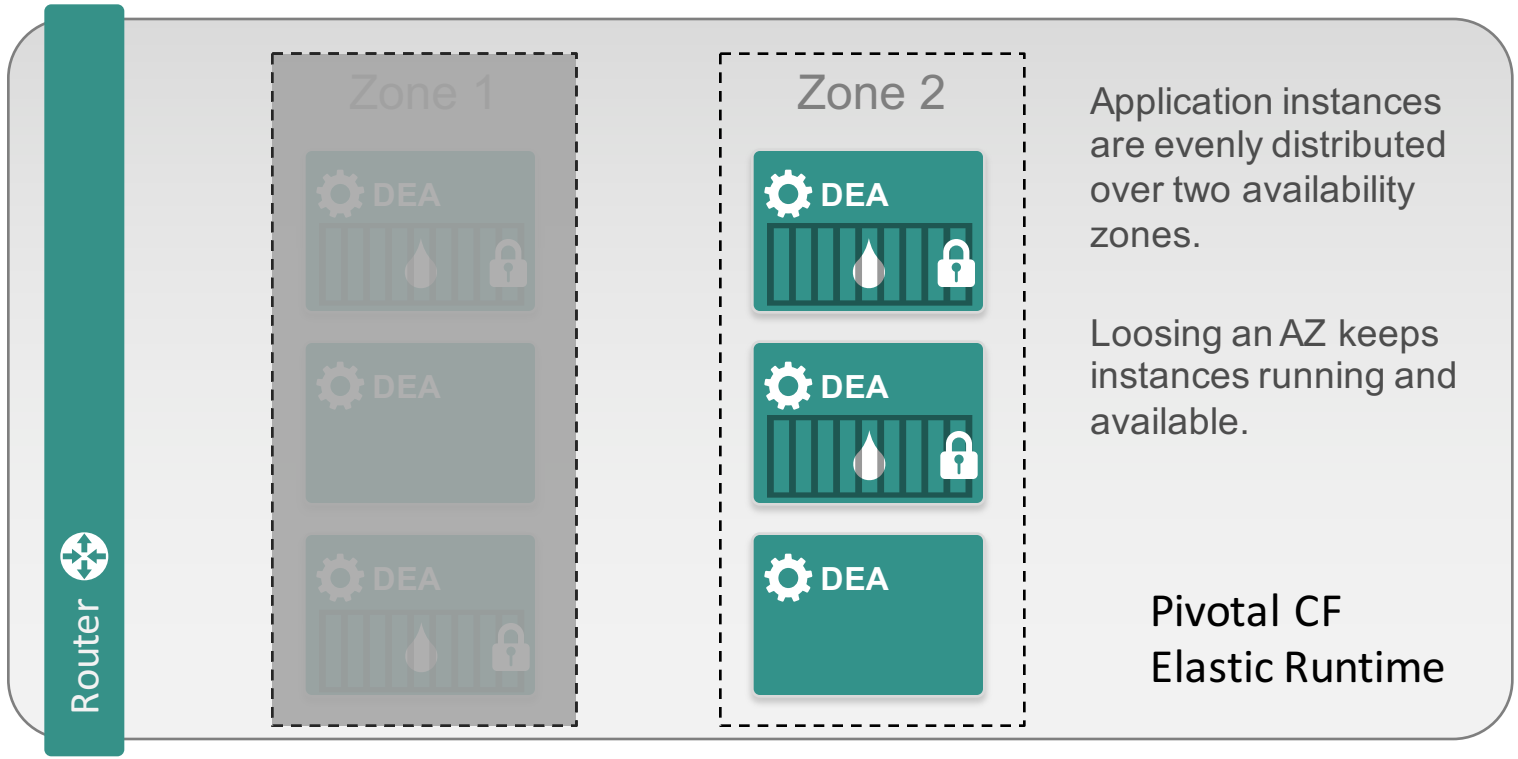
Multiple Availability Zones for HA requirements

- Application and the Platform itself are automatically balanced across availability zones
  - Enhanced availability for applications
  - Tolerate significant infrastructure failures with continuous availability



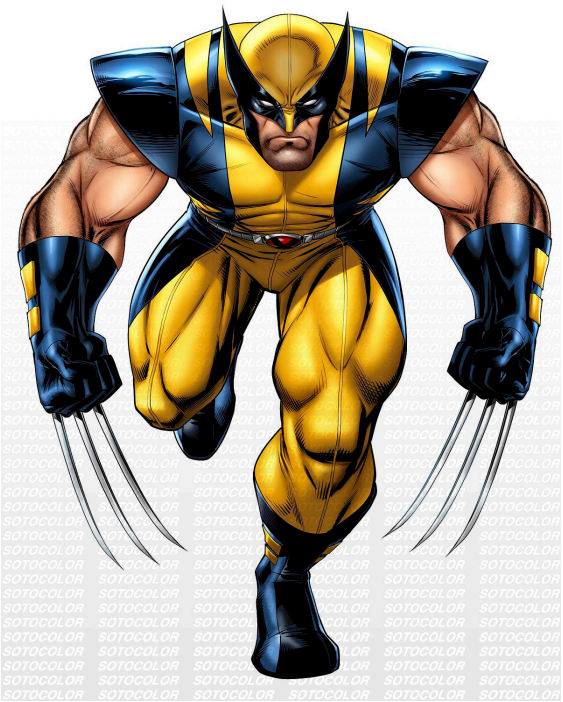
Pivotal

Application Instances and Availability Zones



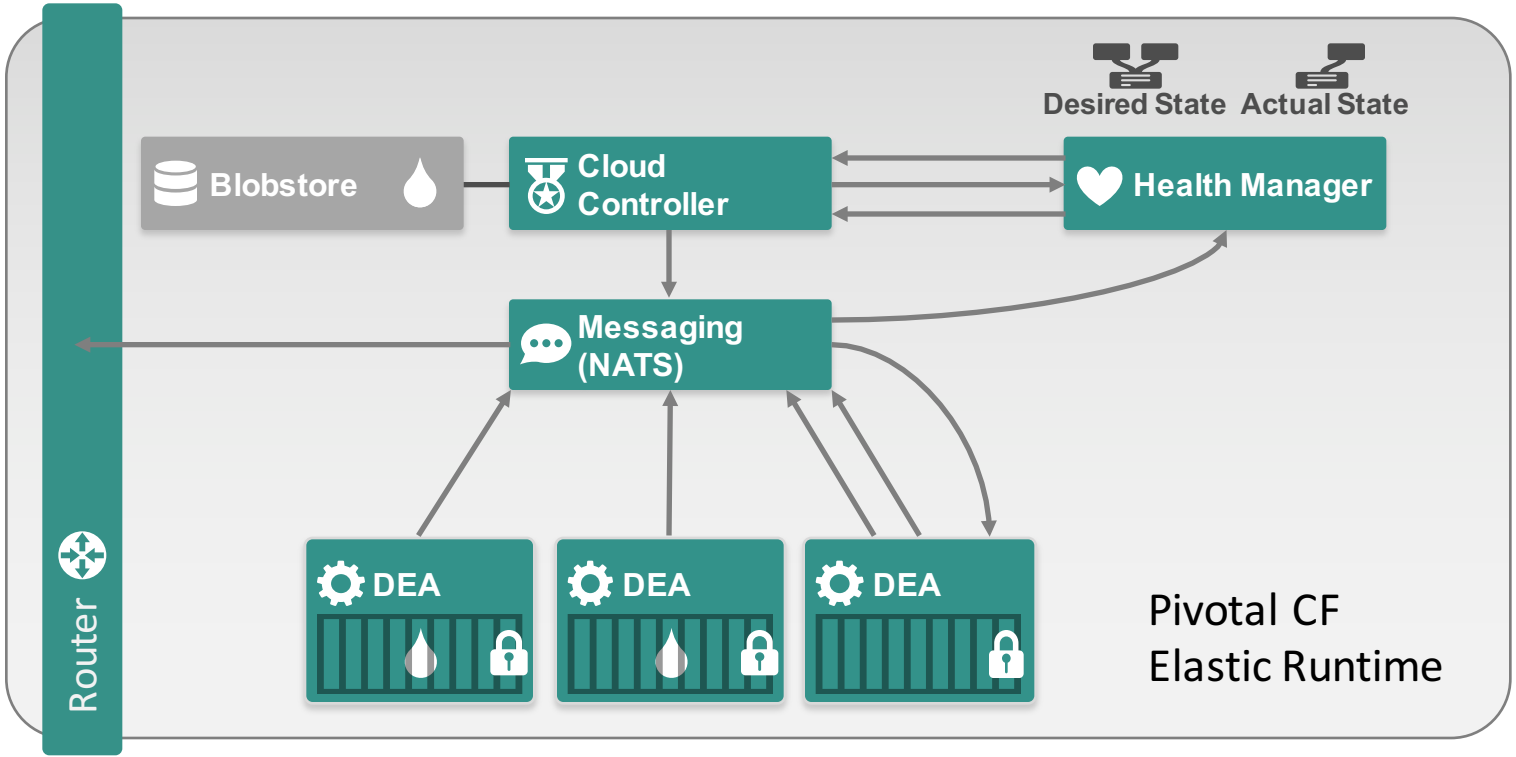
Pivotal

Demo #4 : Self Healing capabilities



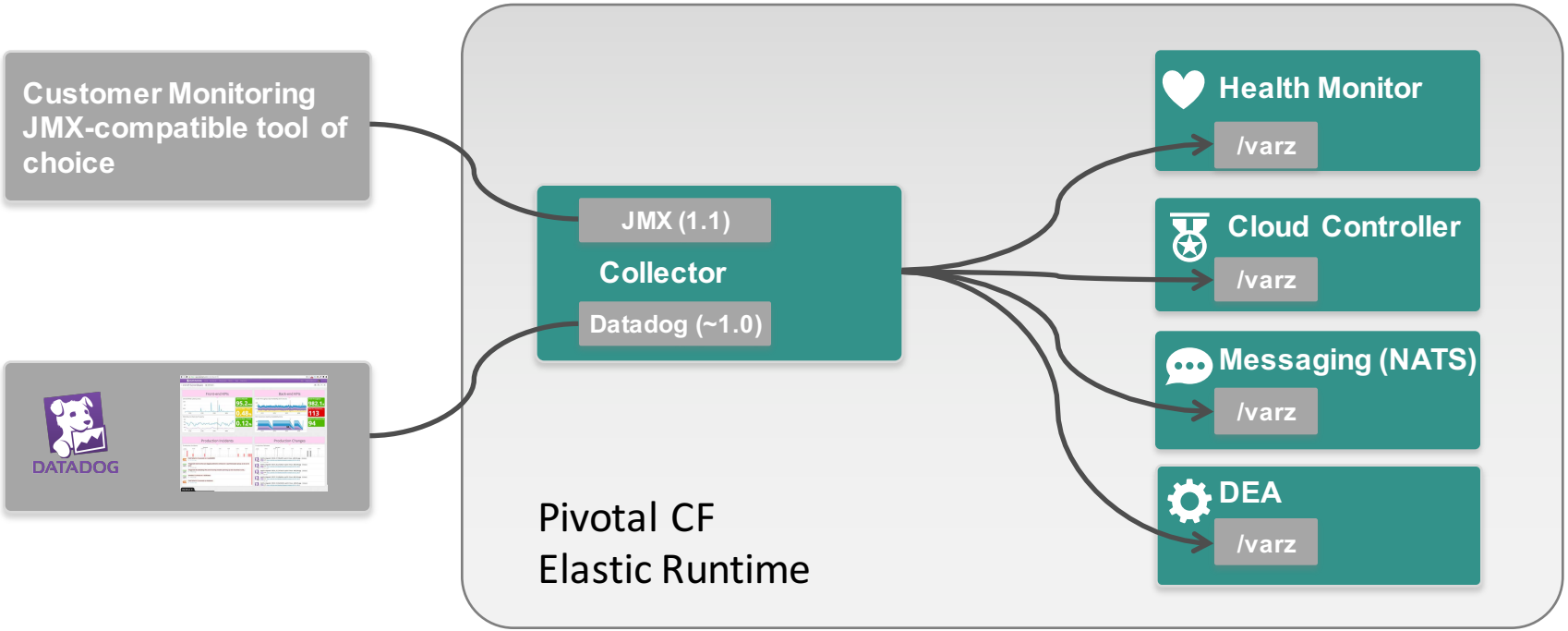
Pivotal

Failed *Application* Instances Replaced

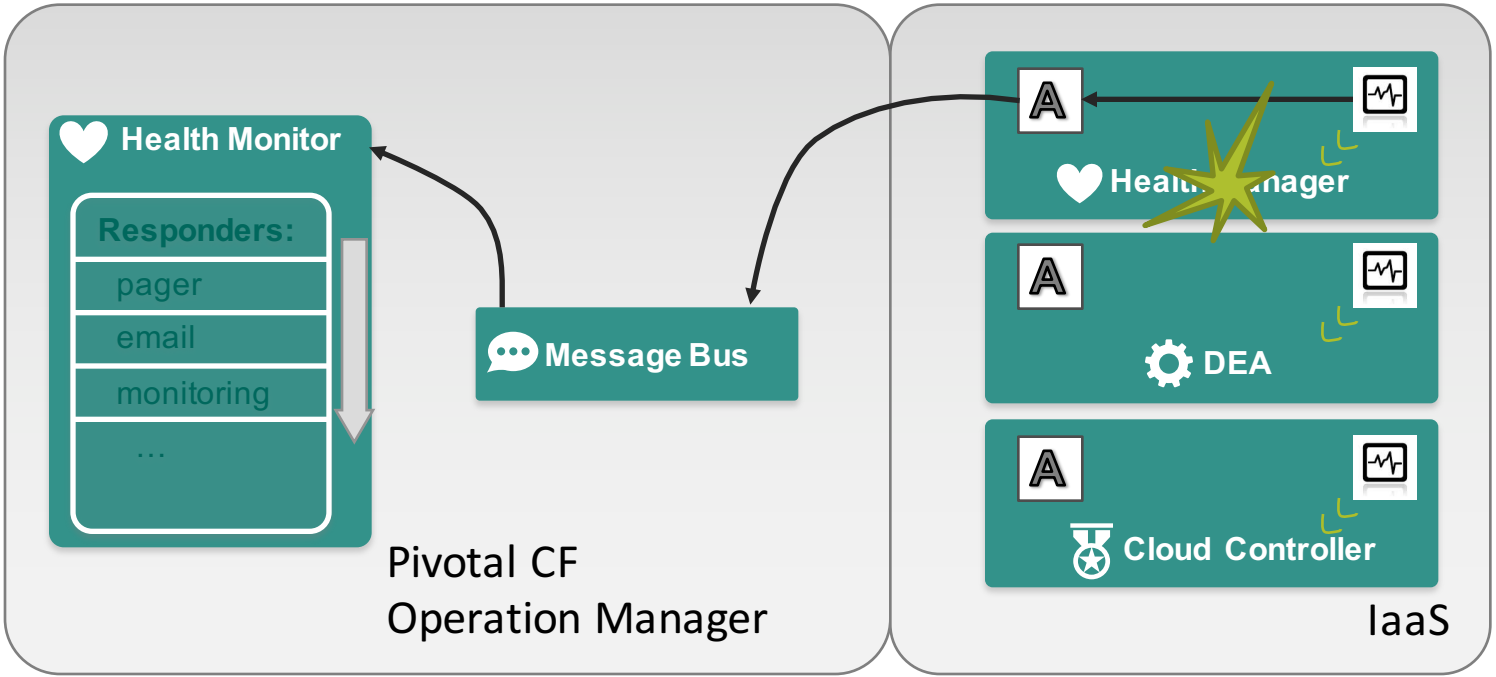


Pivotal

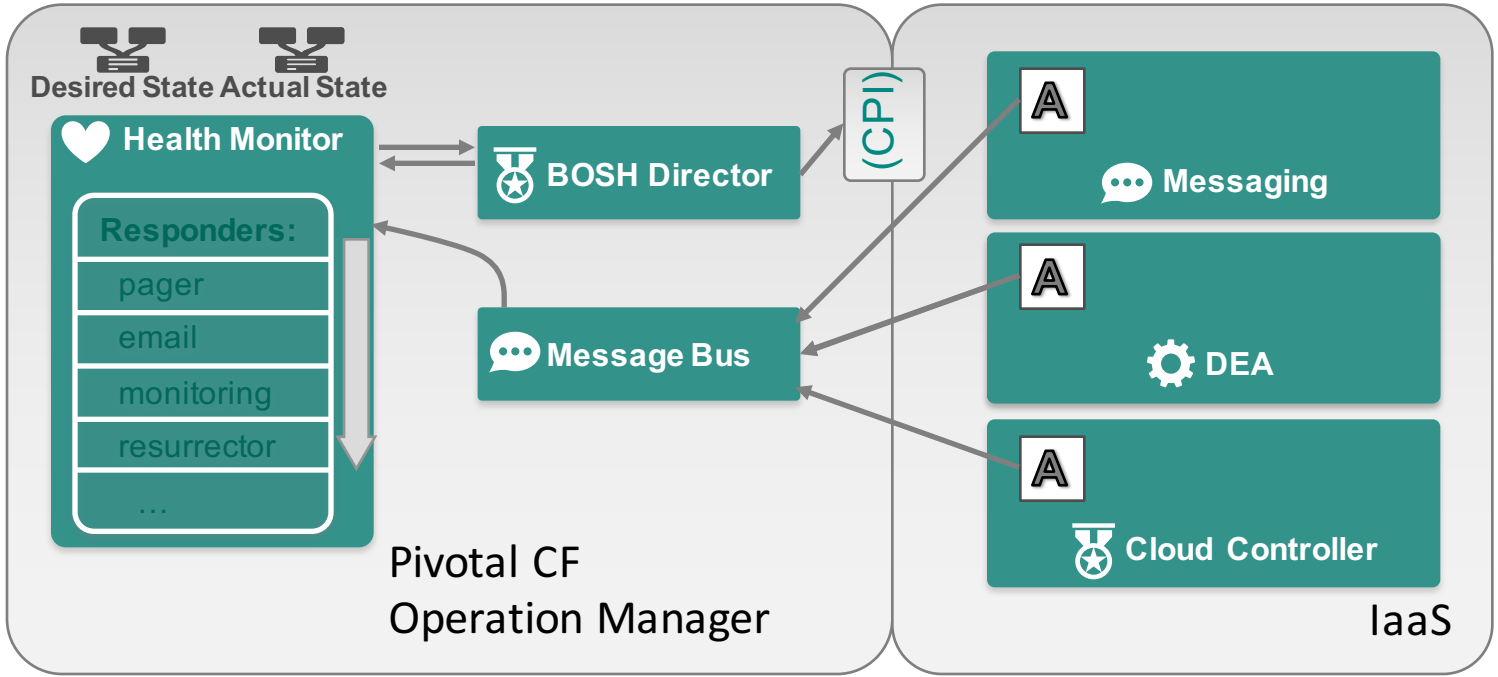
Monitoring CF Components



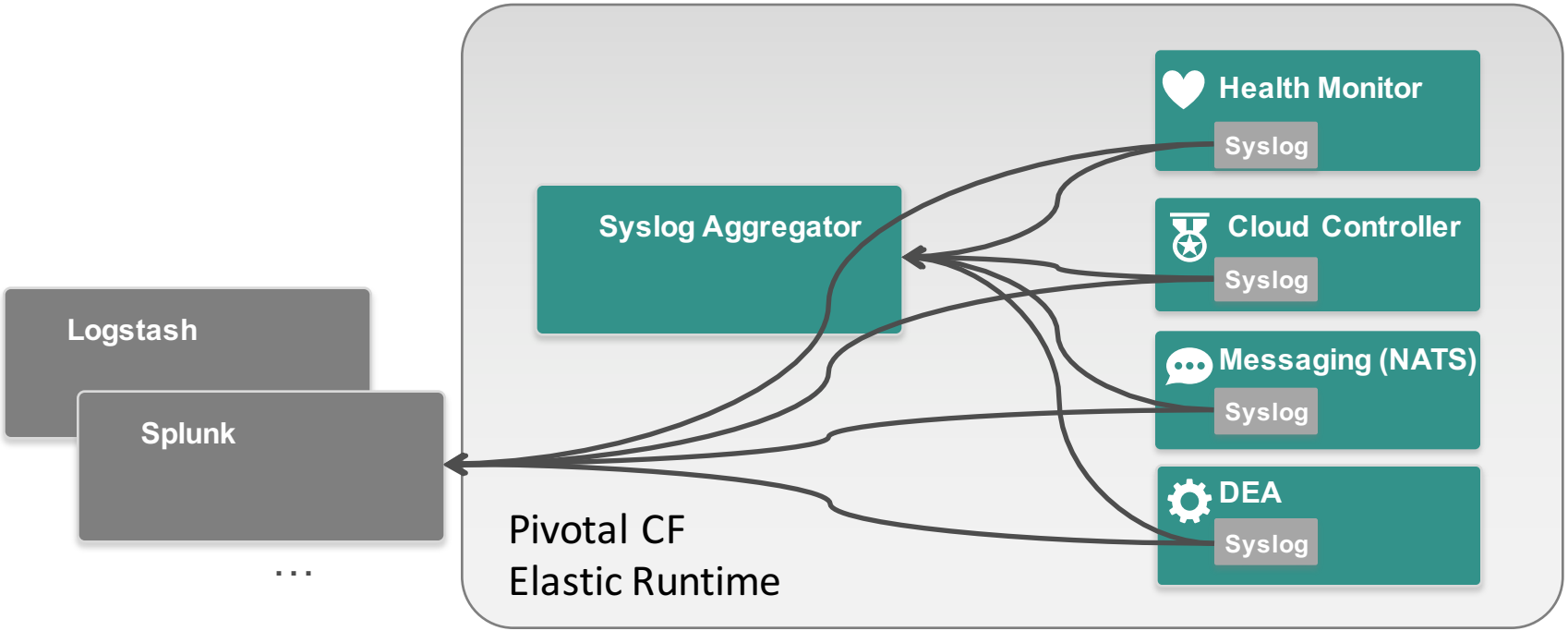
Monitoring Processes *(Elastic Runtime Example)*



Monitoring VMs *(Elastic Runtime Example)*



Log Aggregation



- Log files from /var/vcap/sys/log
- Support for external syslog endpoints in PCF 1.2

Pivotal

Security

Access Control, Application Security Groups and Identity Management

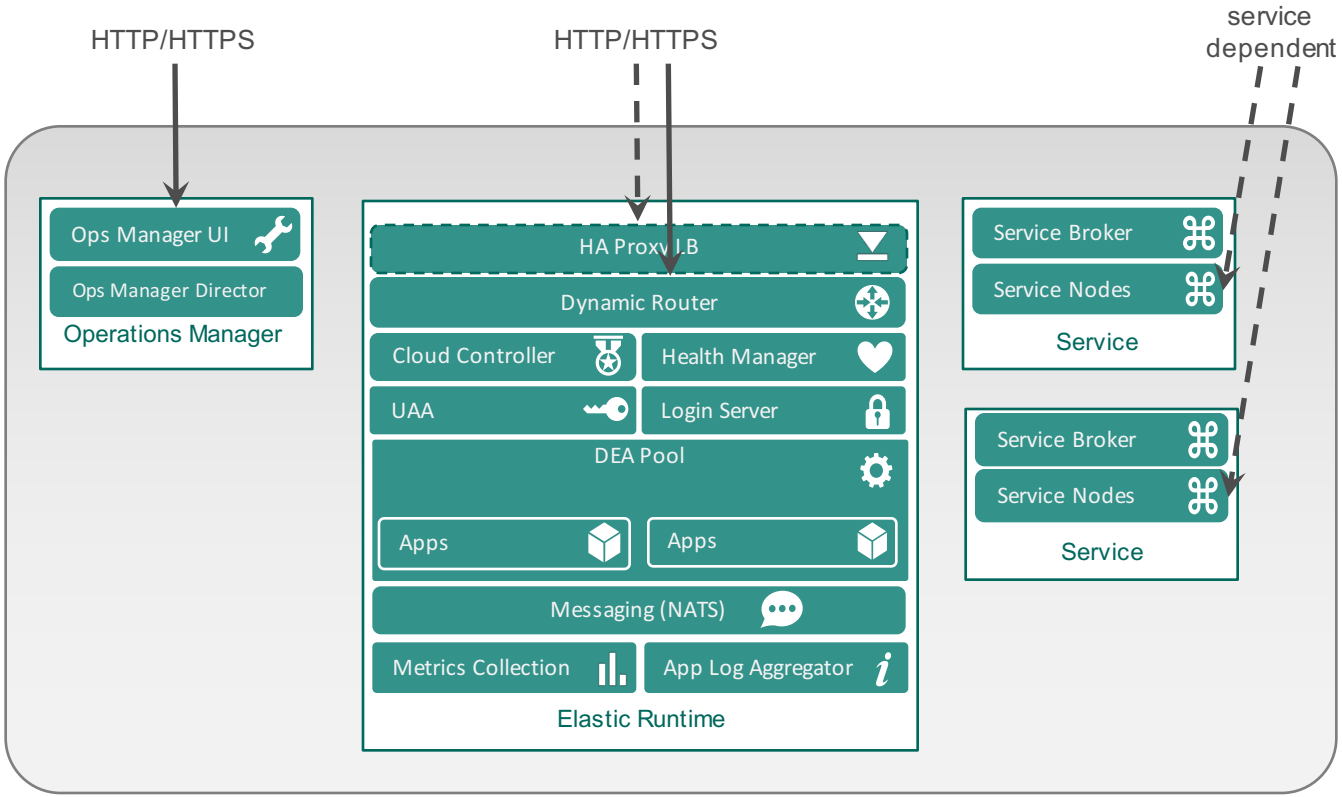
Pivotal

System Boundaries

Minimal Pivotal CF network access

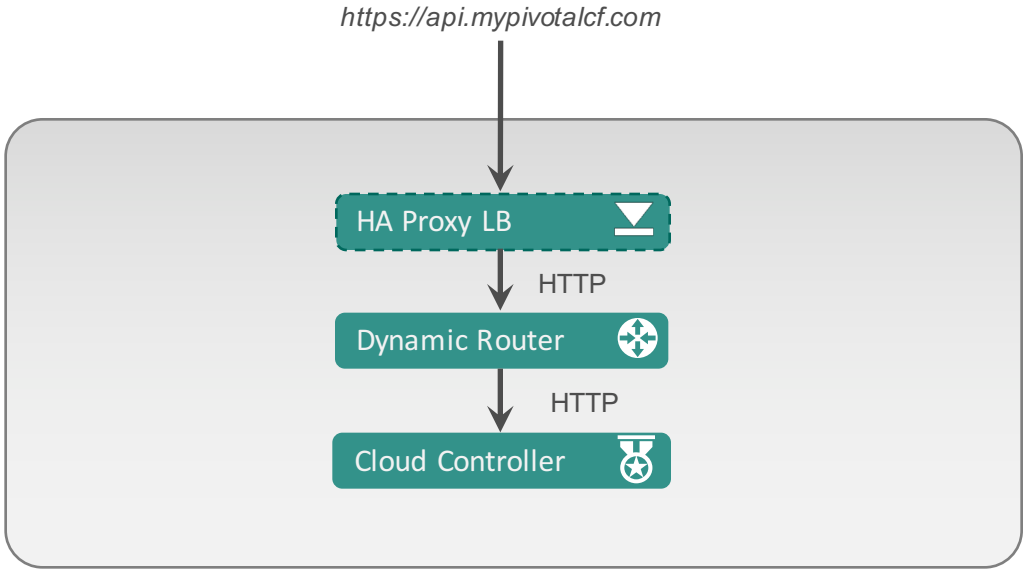
allows PCF to be easily deployed on a VLAN or behind a firewall

reduces surface area for vulnerabilities



API Access

API access (app management, service management, org/space management, etc.) is routed to Cloud Controller via HTTP/HTTPS

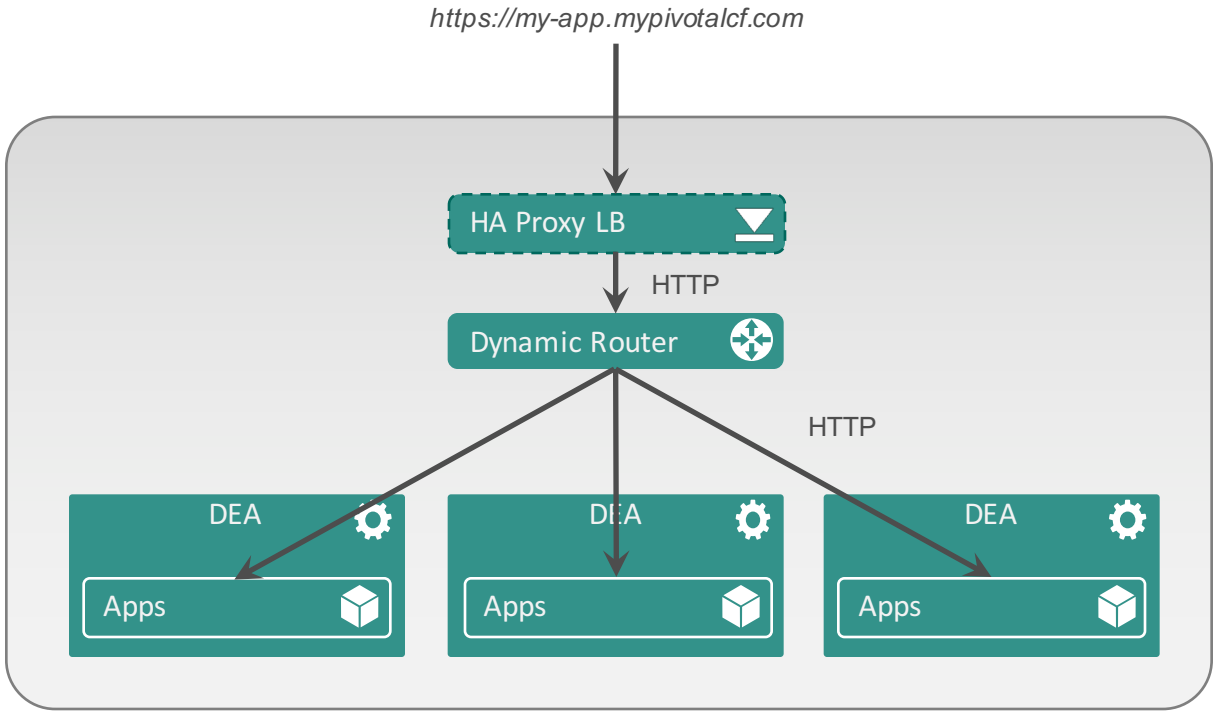


Pivotal

Application Access

Application access is routed directly to an application instance

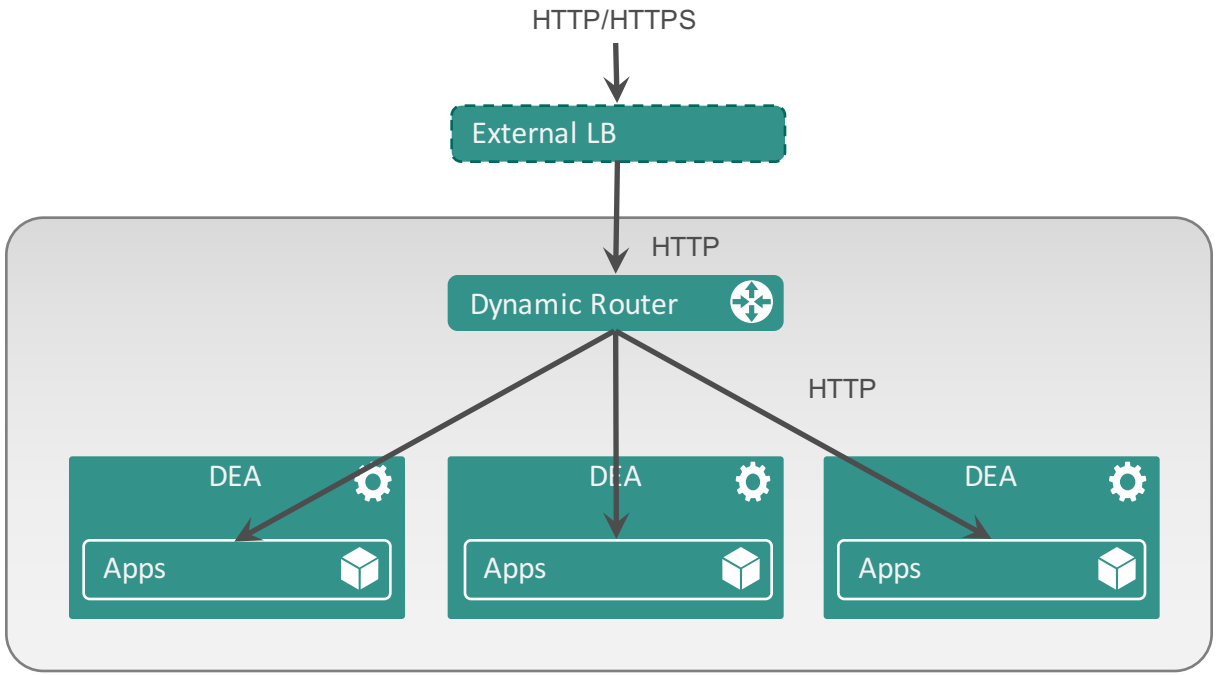
SSL is terminated at the HA Proxy load balancing layer; all internal PCF traffic is trusted HTTP



External Load Balancer

HA Proxy can be replaced with an external Load Balancer

SSL is terminated at the Load Balancer

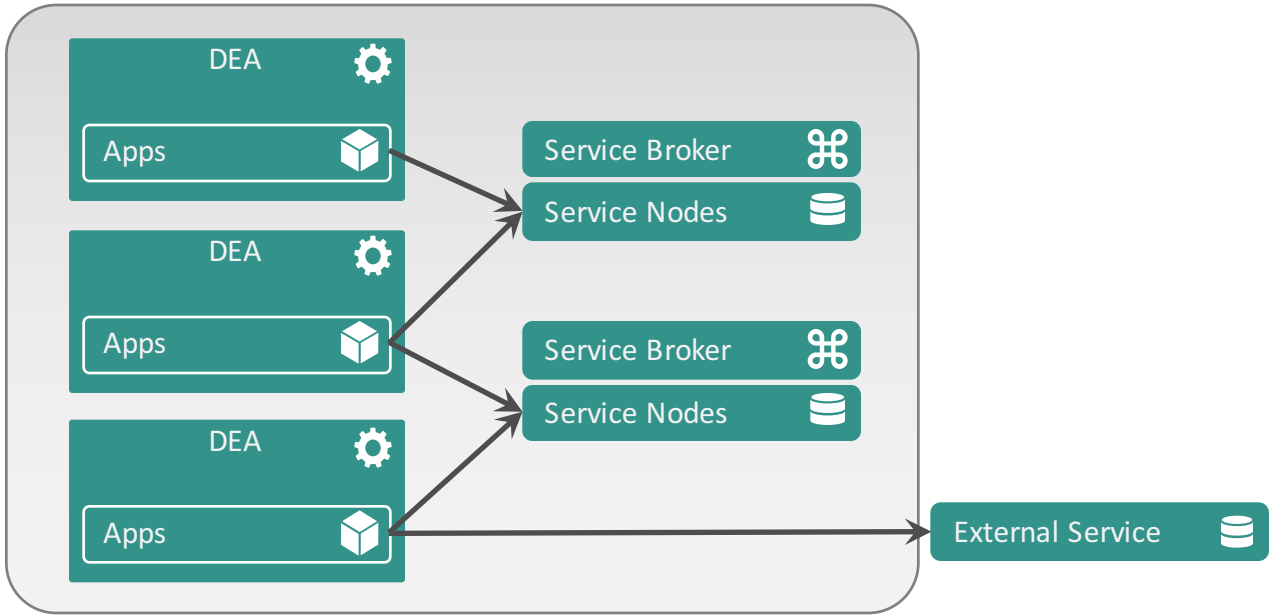


Pivotal

Service Access

Applications connect directly to managed services via assigned addresses and ports

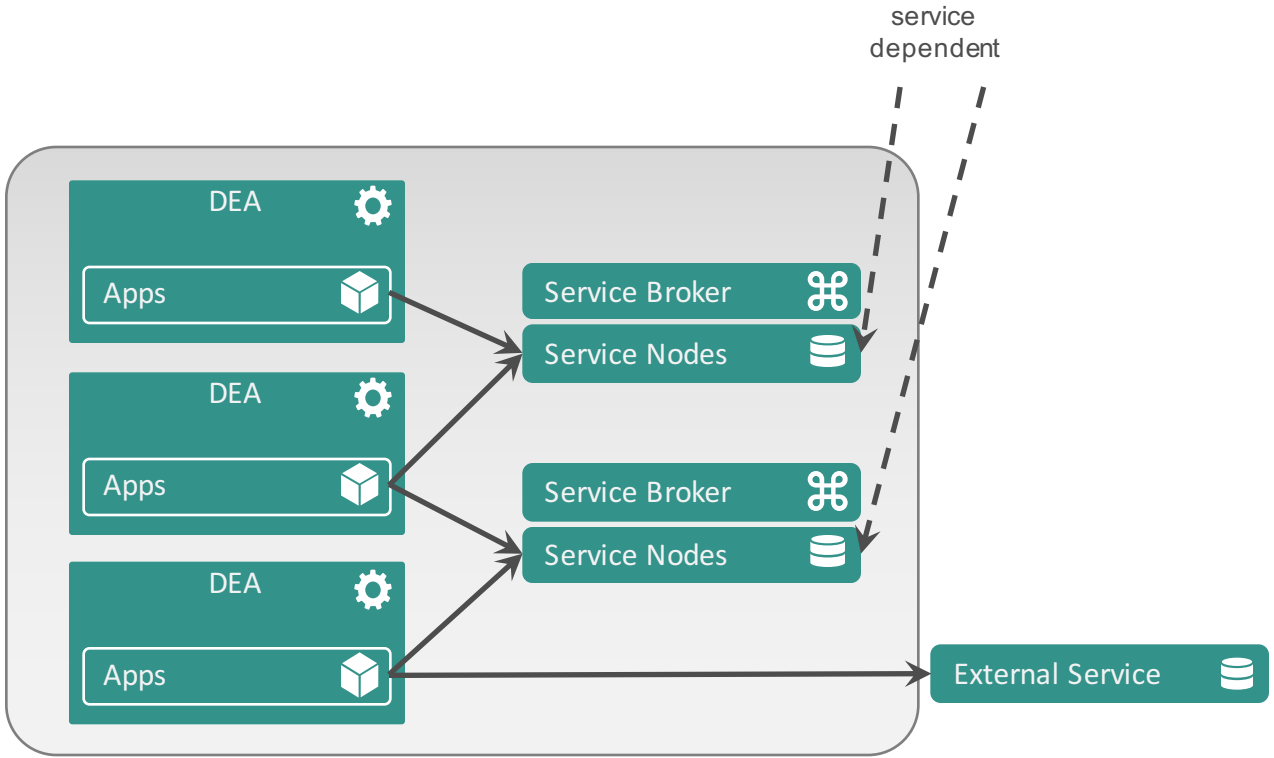
Applications can access “user provided” services outside of the PCF VLAN



Pivotal

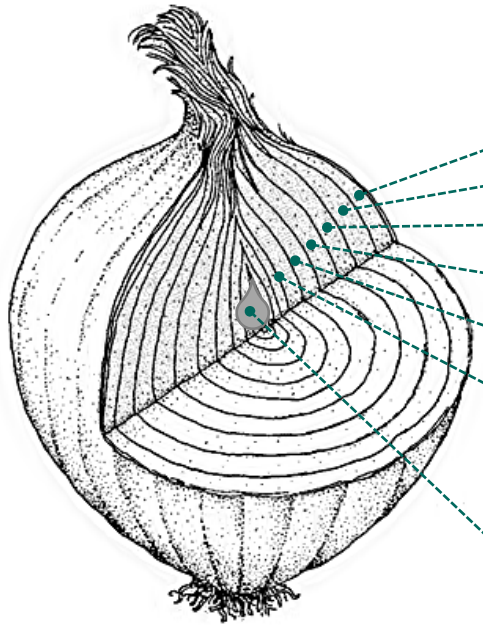
Service Access

- Users can access managed services from outside the PCF VLAN as allowed by firewall rules
  - ports are dependent on the service
- Some services (e.g. RabbitMQ expose dashboard UIs on additional ports



Pivotal

Security Groups – A Layered Approach



Network Edge

Hardware Firewalls

IaaS Security Groups

CF BOSH
Default Security Rules

Elastic Runtime
Default Security Rules

CF Application
Security Groups

My Application

Pivotal

Security Groups – Highlights

- Outbound firewall rules to restrict network traffic to applications
- A set of whitelist rules in three targets
  - All running application (“Global Running”)
  - All application in staging mode (“Global Staging”)
  - Specific groups of applications (“Space”)
- Rules are automatically applied at the app-container creation
  - Result in IPTABLES rules applied to the virtual network interface used by application containers
  - The rule at the bottom of the chain is REJECT

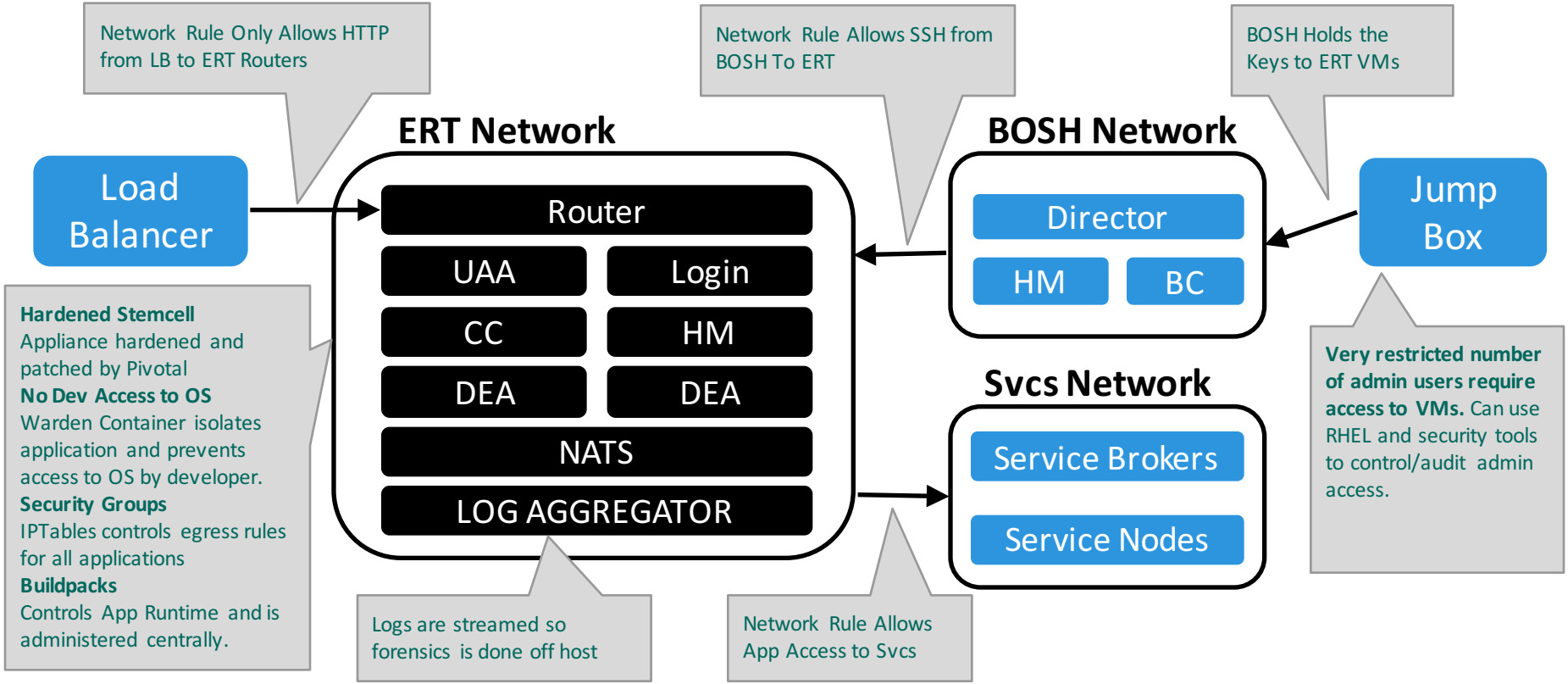
Pivotal

Security Group - Example

```
pivotal-guest-71:twitter-sentiment administrator$ cf security-group my-dev-sec-group
Getting info for security group my-dev-sec-group as admin
OK

Name     my-dev-sec-group
Rules
         [
                  {
                           "destination": "0.0.0.0/0",
                           "ports": "53",
                           "protocol": "tcp"
                  },
                  {
                           "destination": "0.0.0.0/0",
                           "ports": "53",
                           "protocol": "udp"
                  }
         ]
```

Pivotal

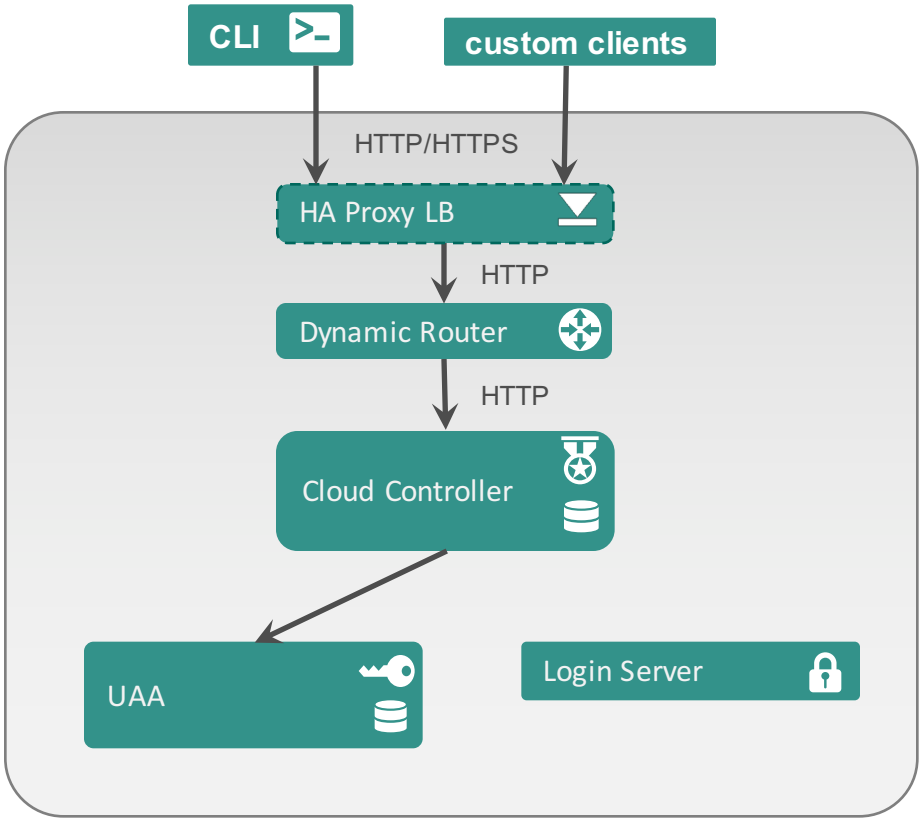
Pivotal CF Security Best Practice



Pivotal

End-User Identity

- Login Server handles authentication
  - by default, stores usernames and passwords in CCDB
  - future releases will support LDAP/AD integration
- UAA is an OAuth2 token server
  - manages access and refresh tokens
- All interactions with the API must include a valid OAuth2 access token



Pivotal

Operator Identity

Operations Manager supports a single username and password for access to operations functions

Pivotal

Operator Identity

Operations Manager creates randomized passwords for access to all managed VMs

VM credentials are visible in the Operations Manager UI

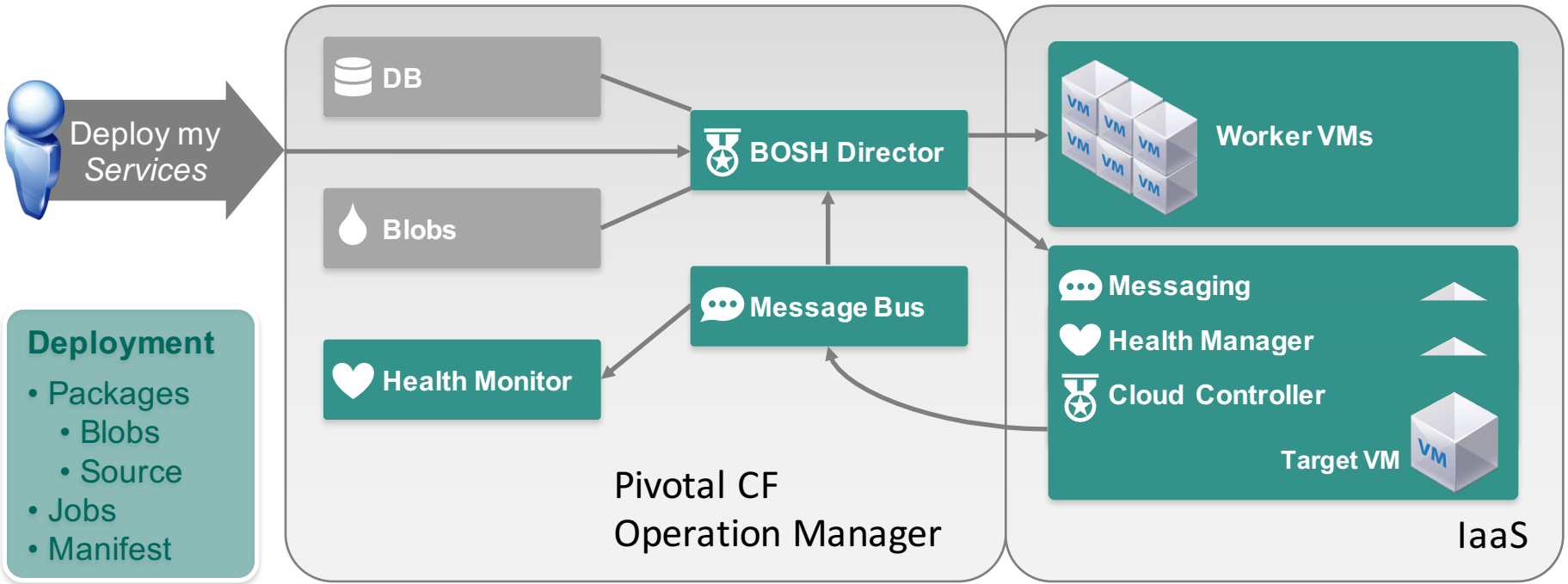
Cloud Controller Database	Vm Credentials	vcap / 56e531a5b88
	Credentials	admin / be1496f7b84858
Cloud Controller	Vm Credentials	vcap / d610de2139
	Staging Upload Credentials	staging_upload_user / 10e8a9da9b19713
	Bulk Api Credentials	bulk_api / a40626299a0a6ee
	Db Encryption Credentials	db_encryption / 0155dcc7d06e0bd
	Encrypt Key	
Clock Global	Vm Credentials	vcap / c2cc41bf52
Cloud Controller Worker	Vm Credentials	vcap / 5547d972b5b
Router	Vm Credentials	vcap / 6a137b41d60
	Status Credentials	router_status / 59453eae513b470
Collector	Vm Credentials	vcap / 23014f7a90d
UAA Database	Vm Credentials	vcap / f41a80501ca
	Credentials	root / f3127d3ba805542
UAA	Vm Credentials	vcap / 8b3fbc5c03f
	Admin Credentials	admin / d4b270780928c0

Pivotal

Operation Manager Behind the Scenes

Pivotal

Operation Manager: Behind the Scenes (BOSH)



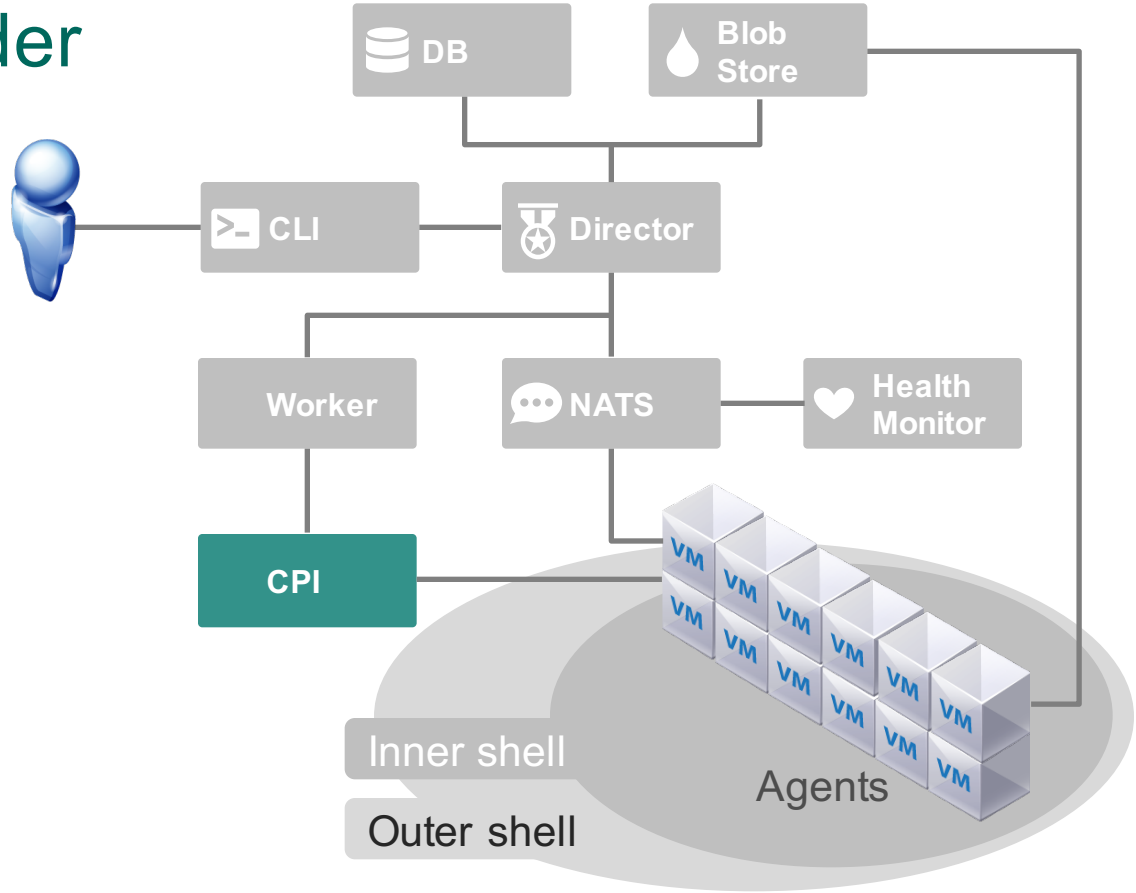
Deployment

- Packages
  - Blobs
  - Source
- Jobs
- Manifest

Pivotal

BOSH: Cloud Provider Interface (CPI)

The core BOSH engine **is abstracted from any particular IaaS**. IaaS interfaces are implemented as plugins to BOSH. Currently, BOSH supports both VMware vSphere and Amazon Web Services. These CPIs allow for automated VM and storage disk provisioning, and network management.



Pivotal

BOSH: Cloud Provider Interface

Stemcell
- create_stemcell(image, cloud_properties)
- delete_stemcell(stemcell_id)

VM
- create_vm(agent_id, stemcell_id, resource_pool, networks, disk_locality, env)
- delete_vm(vm_id)
- reboot_vm(vm_id)
- configure_networks(vm_id, networks)

Disk
- create_disk(size, vm_locality)
- delete_disk(disk_id)
- attach_disk(vm_id, disk_id)
- detach_disk(vm_id, disk_id)

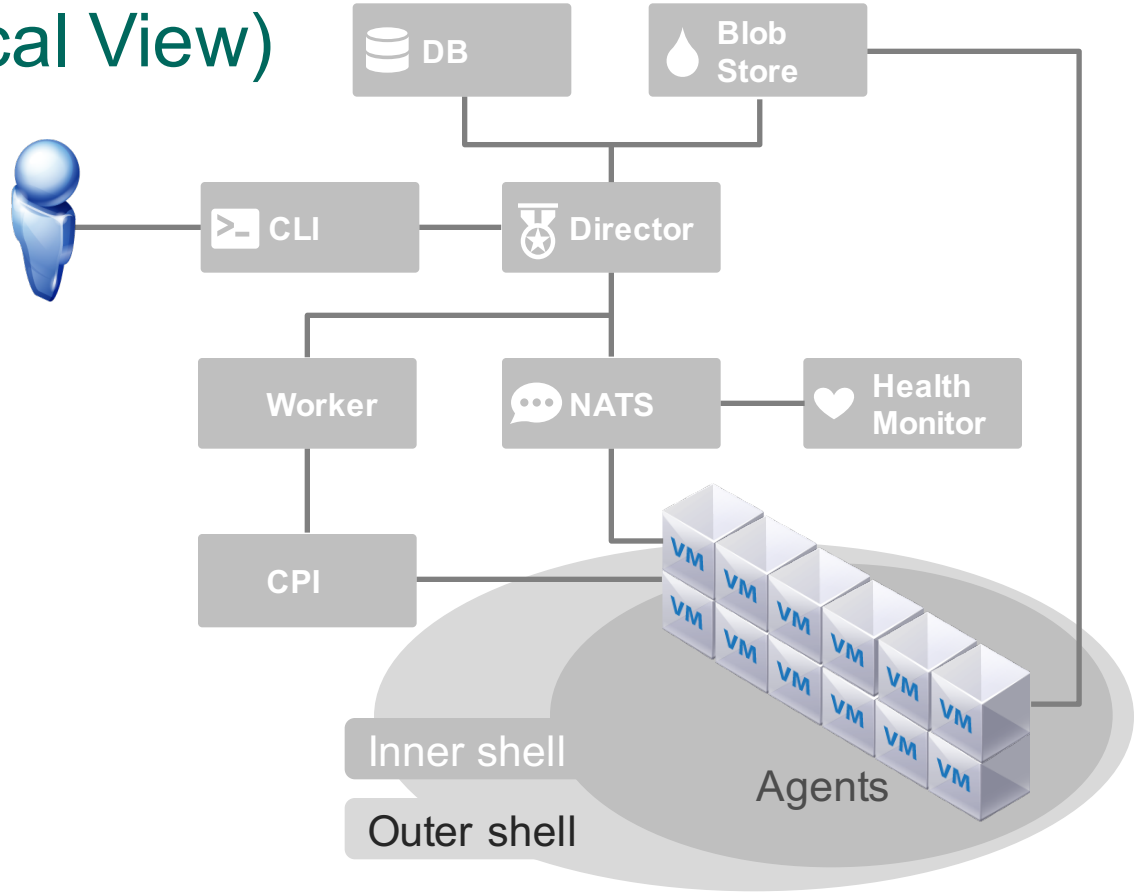
Pivotal

Ops Manager (Logical View)

Deploys and manages large scale distributed systems. **BOSH** provides the means to go from deployment (i.e., Chef/Puppet) to VM creation and management (i.e., cloud CPI). It includes interfaces for vSphere, vCloud, AWS and OpenStack. Additional CPI can be written for alternative IaaS providers.

Key Elements:

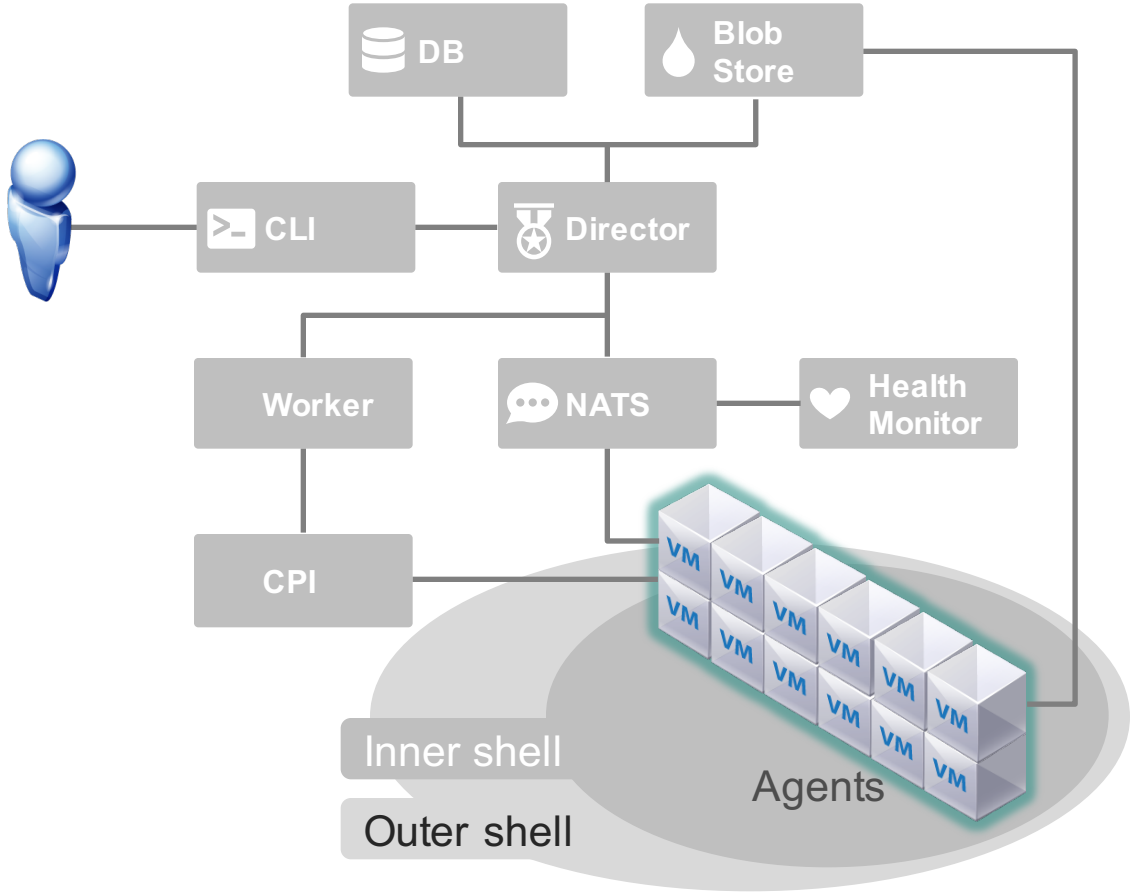
- CLI
- Director
- Blobstore
- Workers
- Message Bus
- Health Monitor
- IaaS CPI
- Agents



Pivotal

BOSH: Stemcells

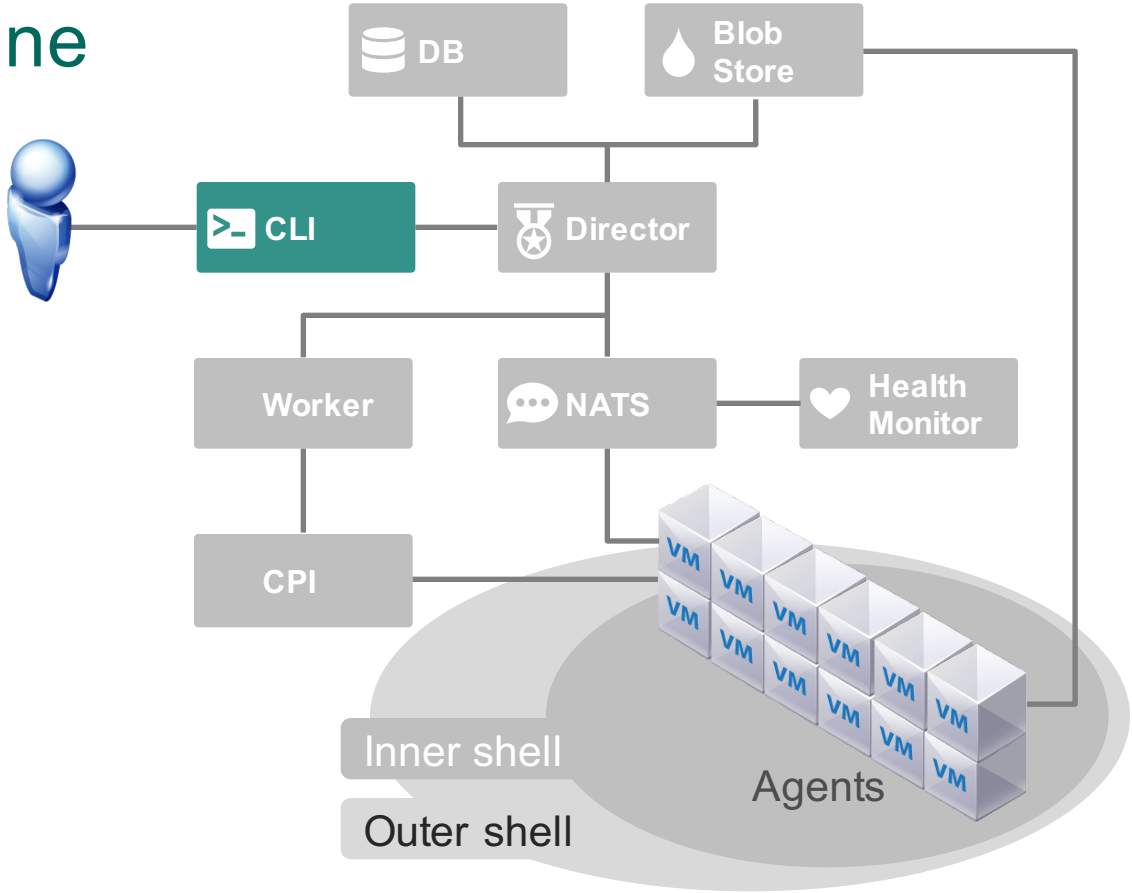
A Stemcell is a VM template with an embedded Agent. Stemcells are uploaded using the CLI and used by the Director when creating VMs through the CPI. When the Director creates a VM through the CPI, it will pass along configurations for networking and storage, as well as the location and credentials for the Message Bus (NATS) and the Blobstore.



Pivotal

BOSH: Command Line Interface

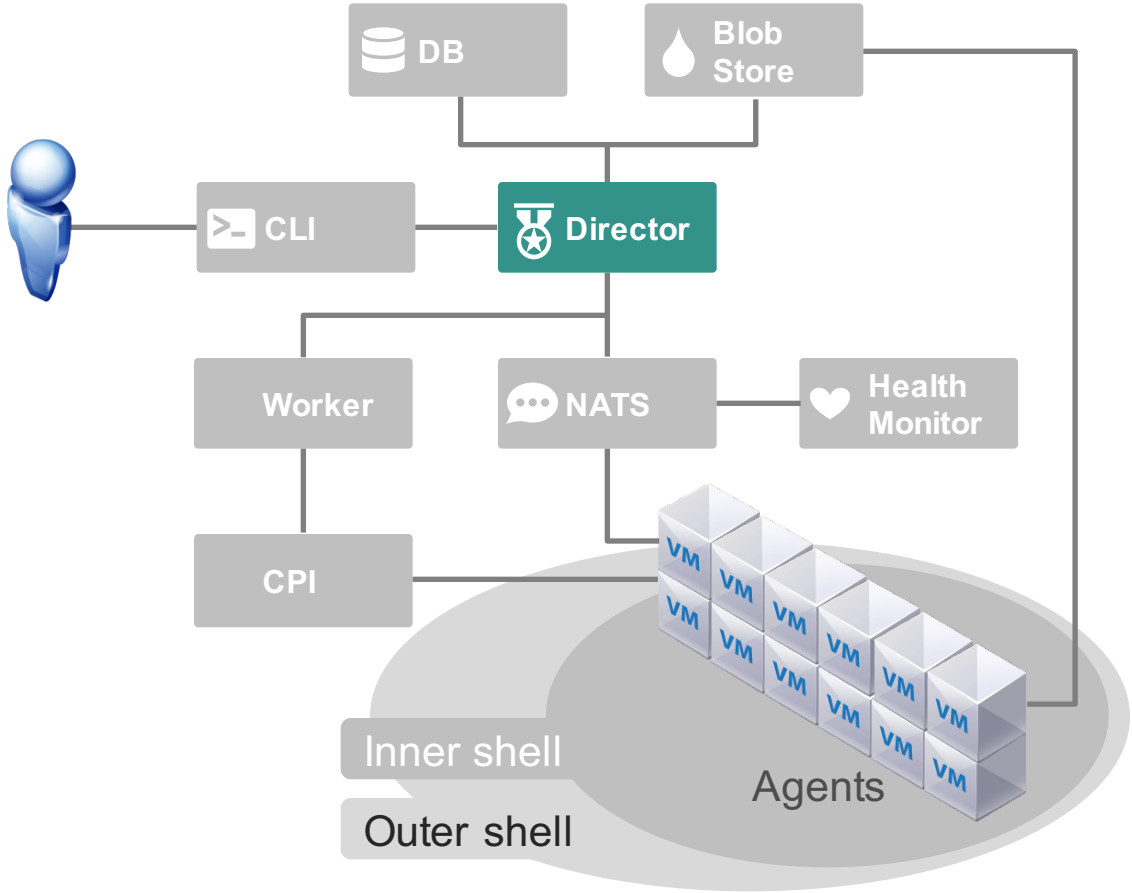
The Command Line Interface is how users interact with BOSH using a terminal session to do a deployment, create and upload releases, and upload ‘stemcells’ (i.e. a VM template with an embedded Agent).



Pivotal

BOSH: Director

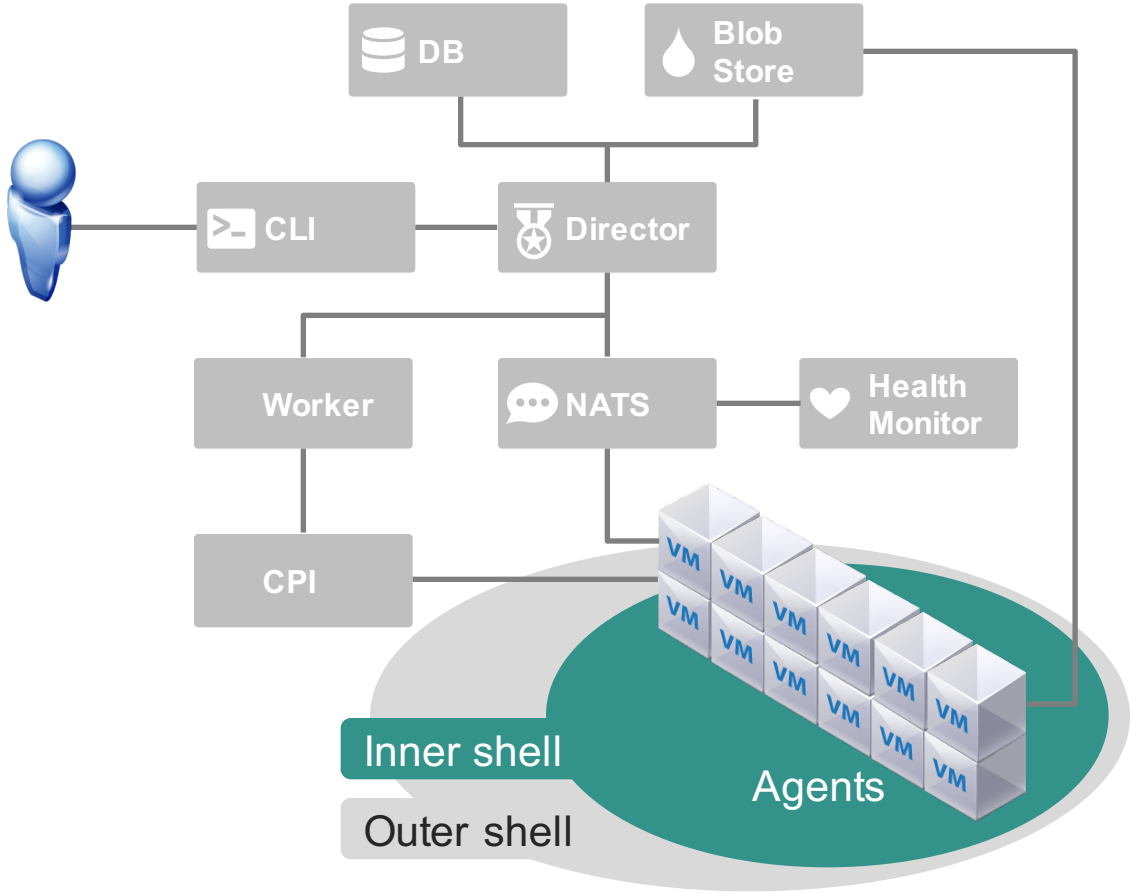
The **core orchestrating** component in BOSH which controls creation of VMs, deployment, and other life cycle events of software and services. Command and control is handed over to the the Director-Agent interaction after the CPI has created resources.



Pivotal

BOSH: Agents

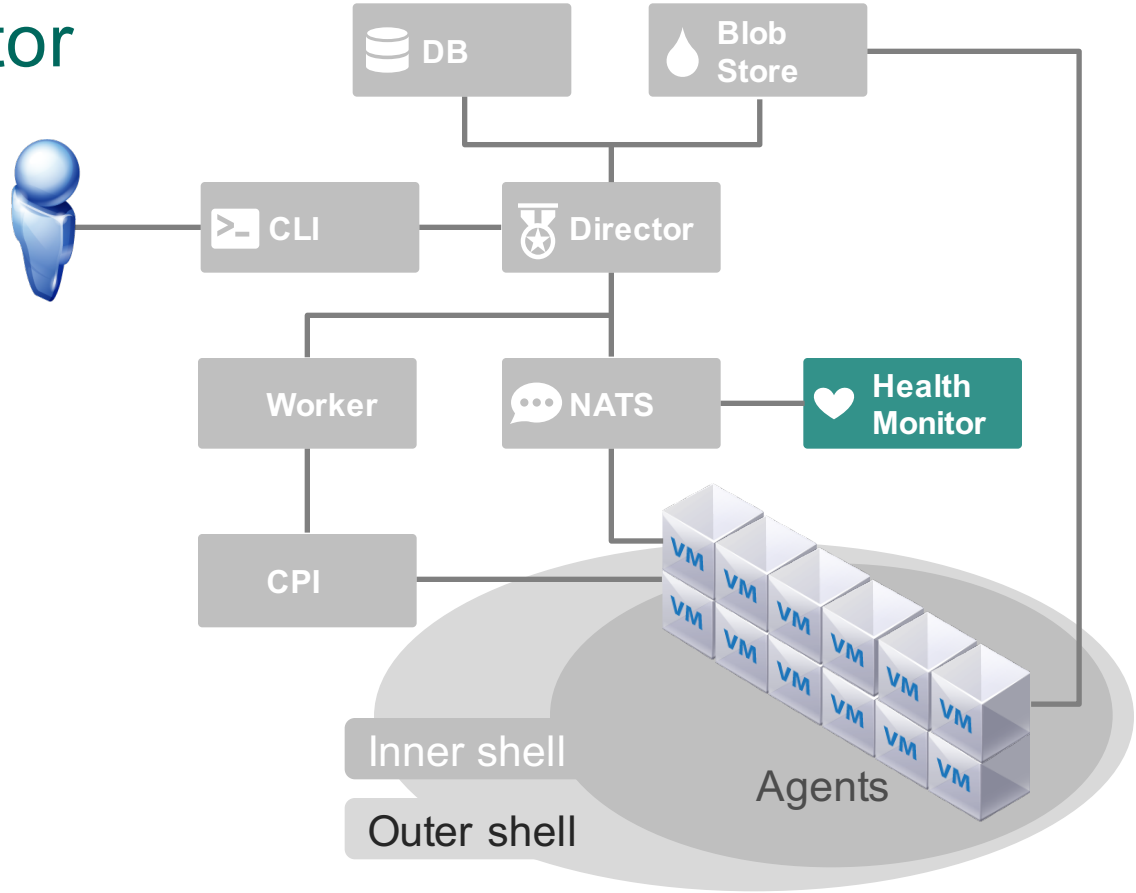
Every VM contains an Agent. Through the Director-Agent interaction, **VMs are given Jobs,** or roles, within Cloud Foundry. If the VM's job is to run MySQL, for example, the Director will send instructions to the Agent about which packages must be installed and what the configurations for those packages are.



Pivotal

BOSH: Health Monitor

Receives health status and life cycle events from Agents and can send alerts through notification plugins (such as email) to operations staff.

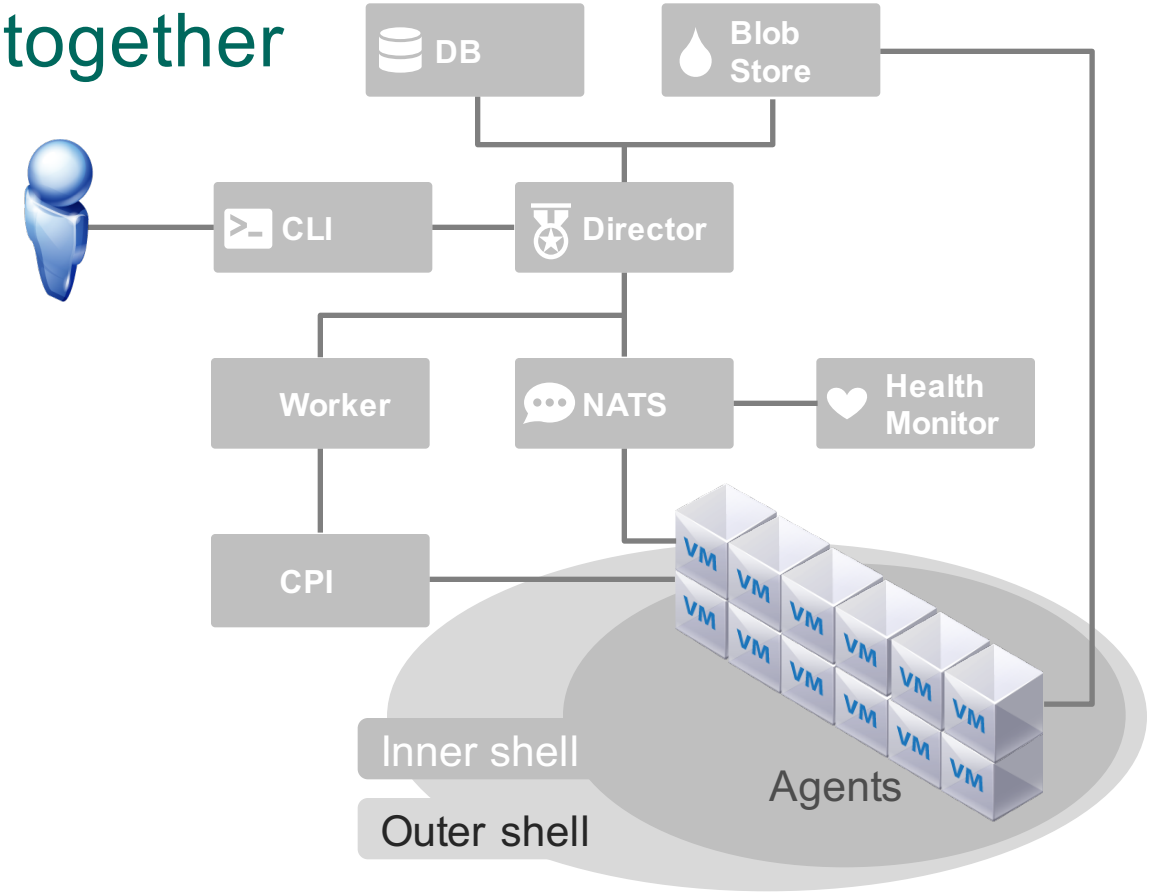


Pivotal

BOSH: Putting it all together

When you deploy Cloud Foundry the following sequence of steps occur:

1. Target a BOSH director using CLI
2. Upload a Stemcell
3. Get a Release from a repo
4. Create a deployment manifest
5. BOSH Deploy Cloud Foundry:
   - Prepare deployment
   - Compile packages
   - Create and bind VMs
   - Pull in job configurations
   - Create needed job instances – this is where things get pushed live



Pivotal

Pivotal CF

Technical Overview

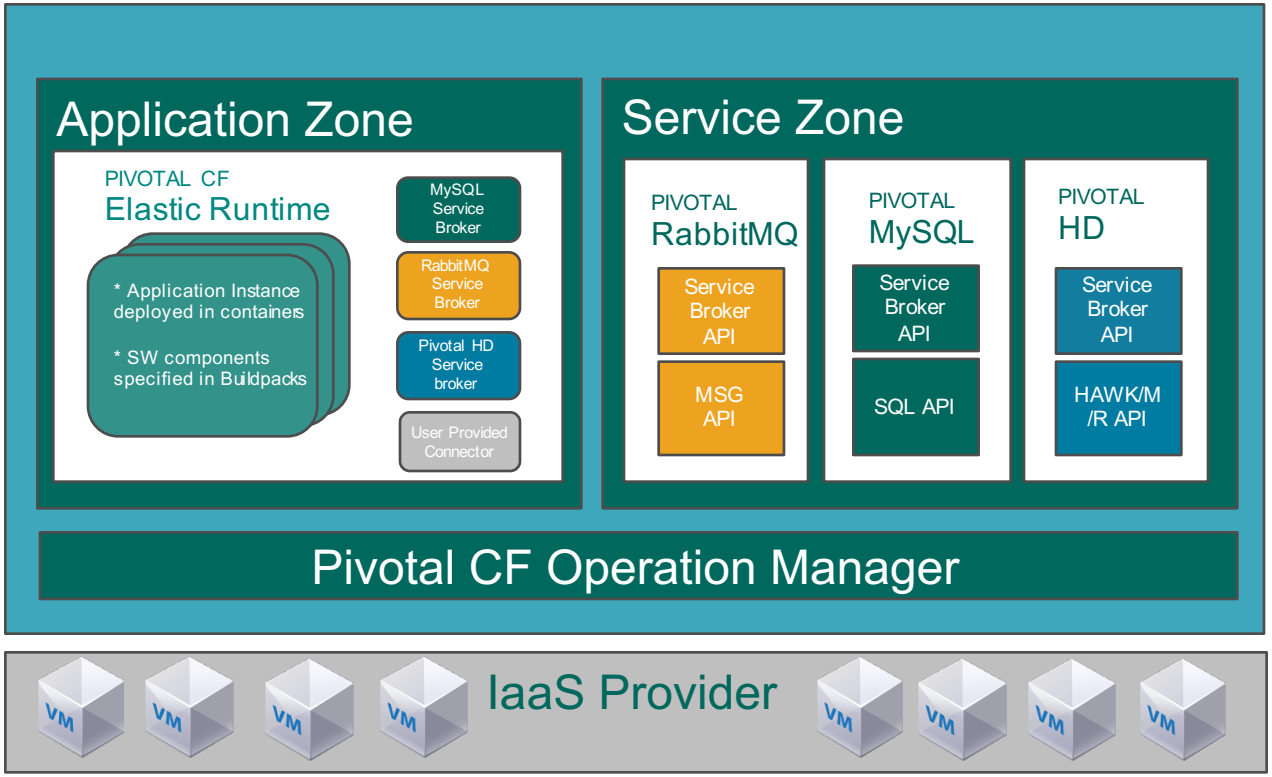
Cloud Foundry Product Group

Thank You.

Pivotal

Additional Slides

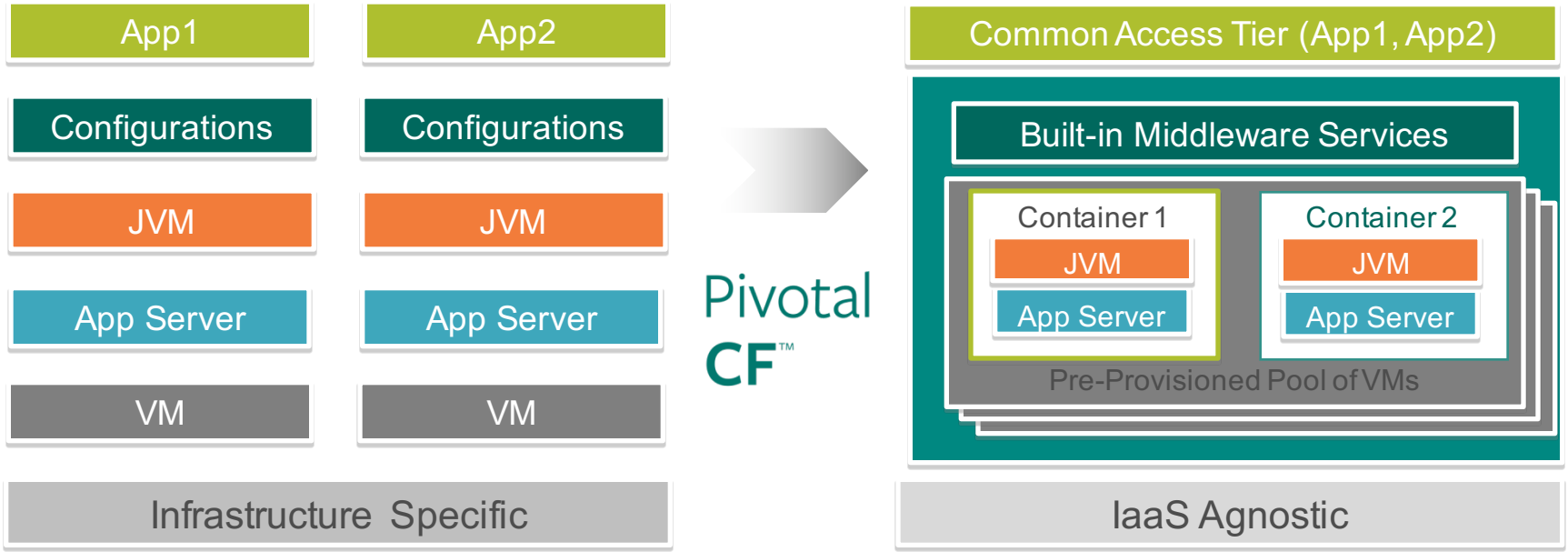
Pivotal CF Packaging



Pre-existing Databases / other services not running on PCF based VMs

Pivotal

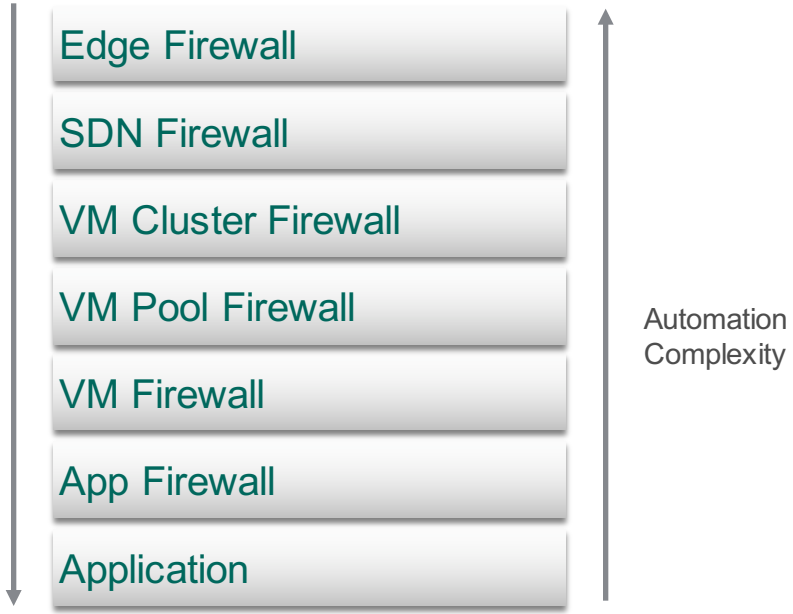
From a VM Centric to Application Centric World



Pivotal

Security Groups – The Future

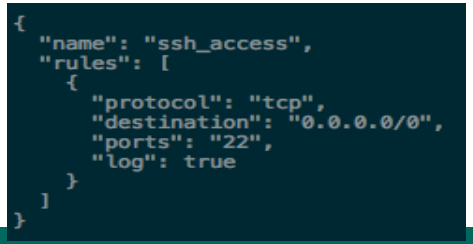
- Work our way up the stack
- Apply Security Groups to more things
- Implement pooling of critical CF resources (aka dea placement pools)
- Automation of SDN firewalling and networking



Pivotal

Security Group Logging – Coming Soon

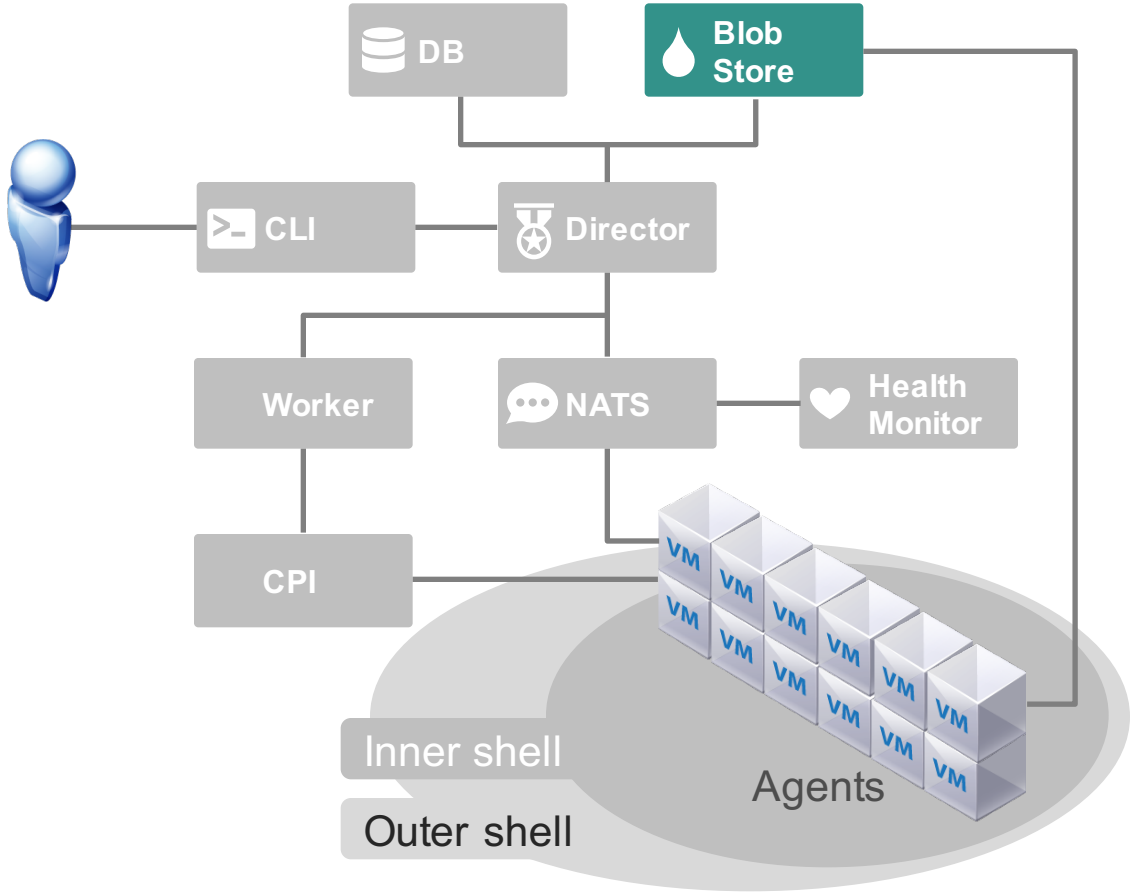
- In newer CF builds (v180+), first packet logging is now supported. By setting the logging attribute to true on a security group rule, the first packet of all outbound connections will be logged to the syslog. These logs will be picked up by the log aggregation service and made available to the CF operator's configured sink. This allows an operator to quickly respond to abuse reports and link a reported target host with an originating application in Cloud Foundry.
- Security Group Log Considerations:
- Every time an application creates an outbound connection that matches the rule, a log line will be added to the syslog.
- Using this feature in a large CF environment will result in a substantial increase to log data being stored.
- While this feature does not log packet content data, it does log metadata around the connection from a user's application. Appropriate updates to an environments terms of use should be considered when enabling this feature.



Pivotal

BOSH: Blobstore

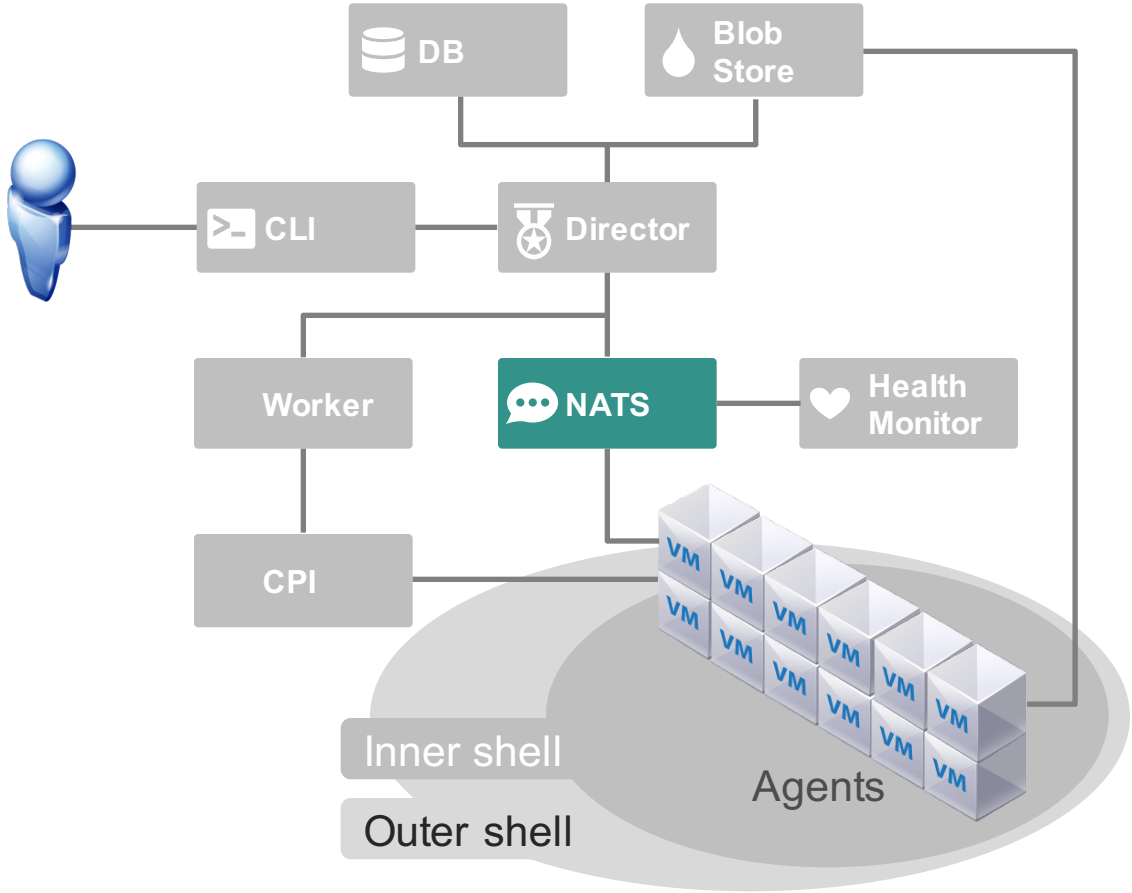
Used to **store the content of Releases, Jobs and Packages** in their source form as well as the compiled image. When you deploy a Release, BOSH will orchestrate the compilation of packages and store the result in Blobstore. When BOSH deploys a Job to a VM, the Agent will pull the specified Job and associated Packages from the Blobstore.



Pivotal

BOSH: NATS

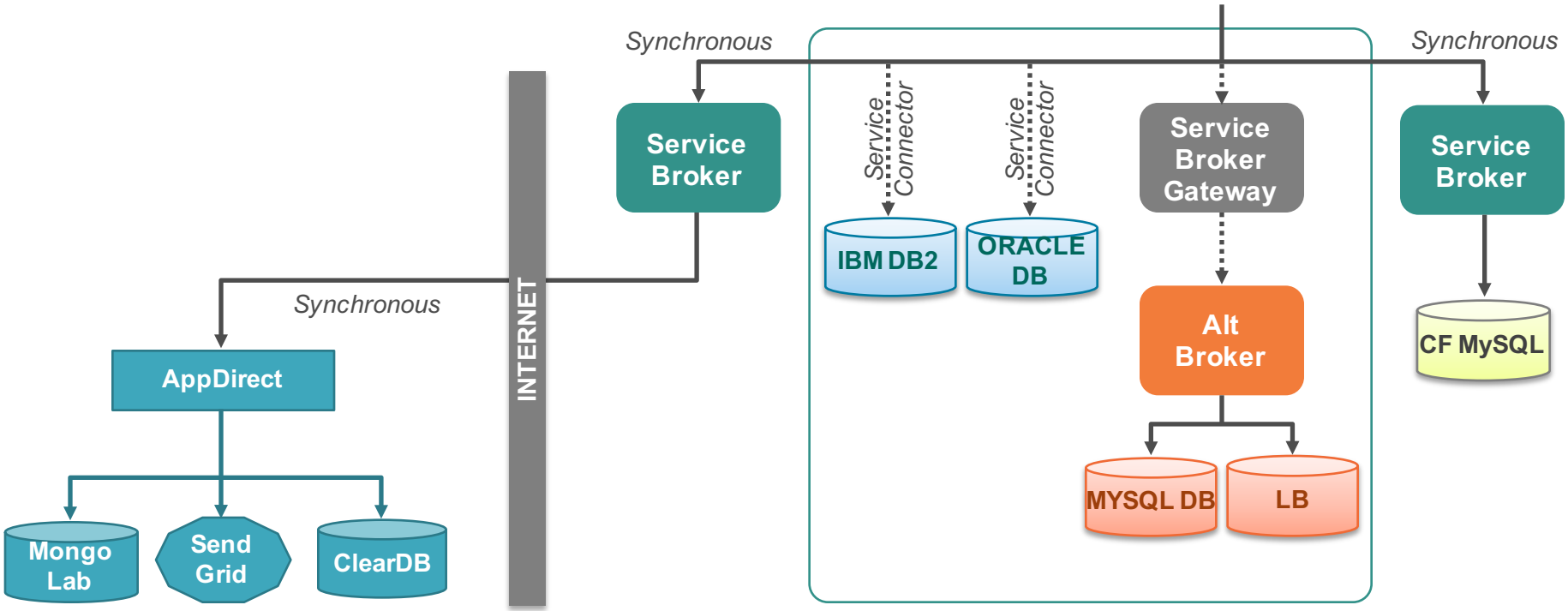
BOSH components use NATS, a lightweight pub sub messaging system, for command and control.



Pivotal

User Provided Service Instances (on-prem example)

Pivotal CF™



Pivotal