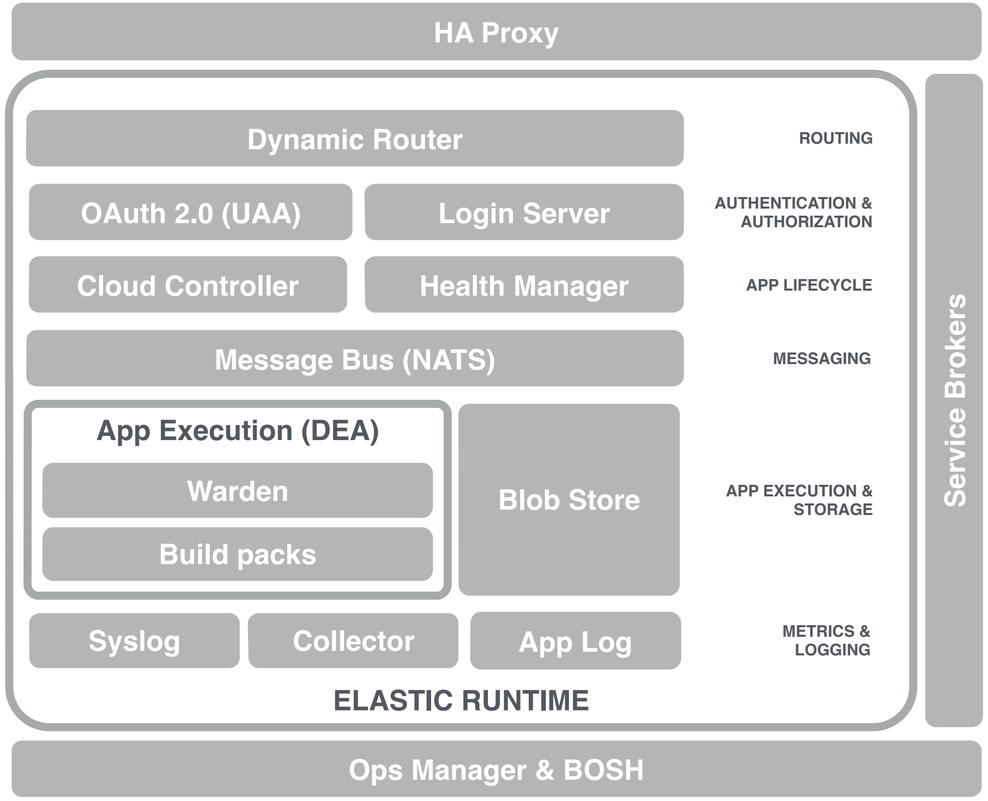
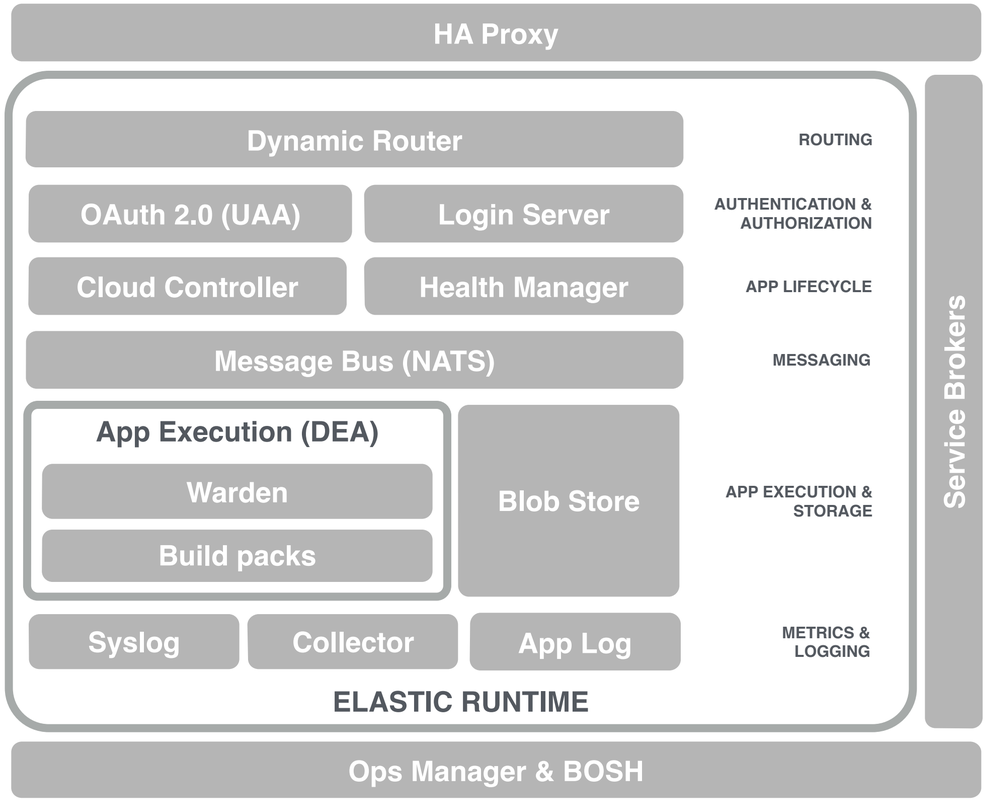
Cloud Foundry Technical Overview



Cloud Foundry Technical Overview



Goal:

To understand the major components of Cloud Foundry and how they contribute to:

- **The Core Tenets of CF:**
  - Developer Agility
  - Operator Agility
  - Robust Services Ecosystem
  - IaaS Independence

- **The 4 levels of High Availability**

Pivotal

Pivotal CF: Cloud Independent Enterprise PaaS

Simple, Developer Friendly Commands & API

- Auto-detect frameworks
- "Push and it works"
  - .WAR
  - Dockerfile
  - .NET
- Simple service binding
- Agile micro-services

Extensible Framework "Buildpack" Architecture

Operational Benefits for Every Application

- Instant Dynamic Routing
- Log Streams & Aggregation
- Access Controls & Policies
- APM and Auto-scaling
- 4 Layers of High Availability
  - *App-Instance*
  - *Availability Zone*
  - *Process*
  - *Virtual Machine*

Built-in and Ecosystem Services

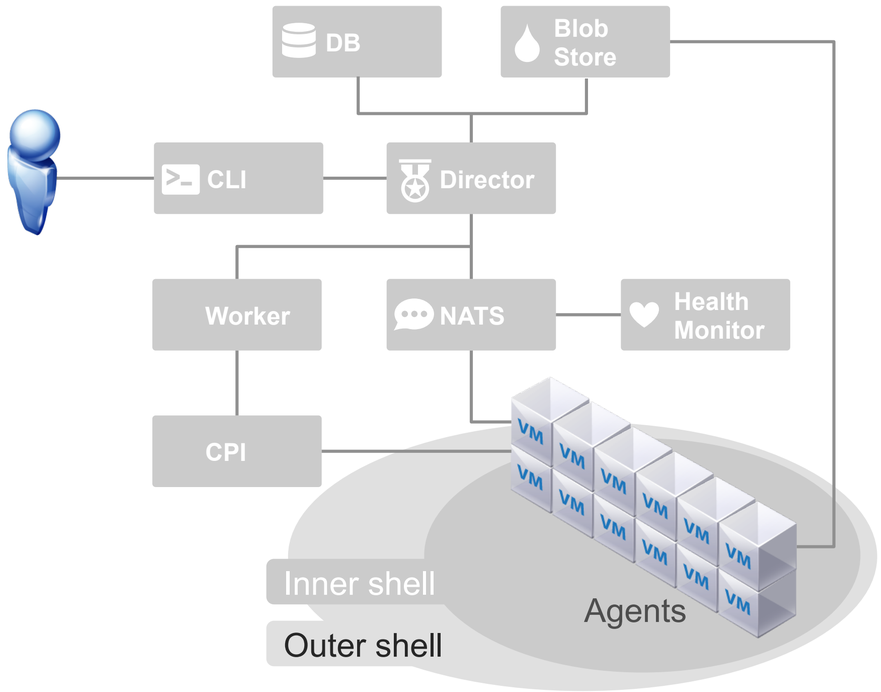
- Elastic Hadoop
- Mobile
  - Push, Sync, API
- MySQL HA
- Redis
- Rabbit MQ
- ElasticSearch
- MongoDB
- Cassandra
- Jenkins (CI)
- PHD
- And More…

Extensible Service Broker Architecture

Deploy, Operate Update, Scale Platform on Any IaaS

vmware · amazon web services™ · openstack · Google Cloud Platform · ….and more

BOSH deploys and manages large scale distributed systems. It provides the means to go from deployment (i.e., Chef/Puppet) to VM creation and lifecycle management. Core to bosh is the ability to execute **Canary-style deployments** with zero downtime.

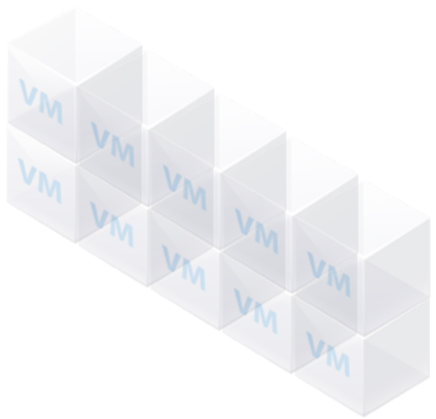


Ops Manager & BOSH

Canary Style Updates

BOSH

v1.0



v1.1

Ops Manager & BOSH

# of Canaries: 2

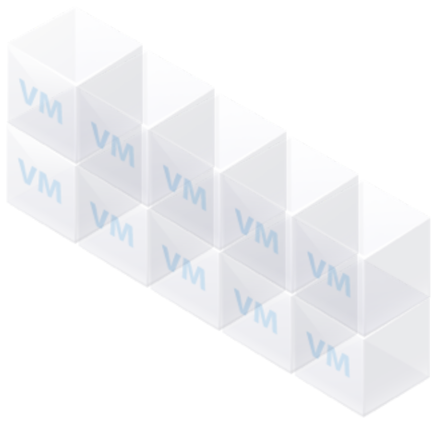
Max in Flight: 2

Pivotal

Canary Style Updates

BOSH

v1.0



v1.1

Ops Manager & BOSH

# of Canaries: 2

Max in Flight: 2

Pivotal

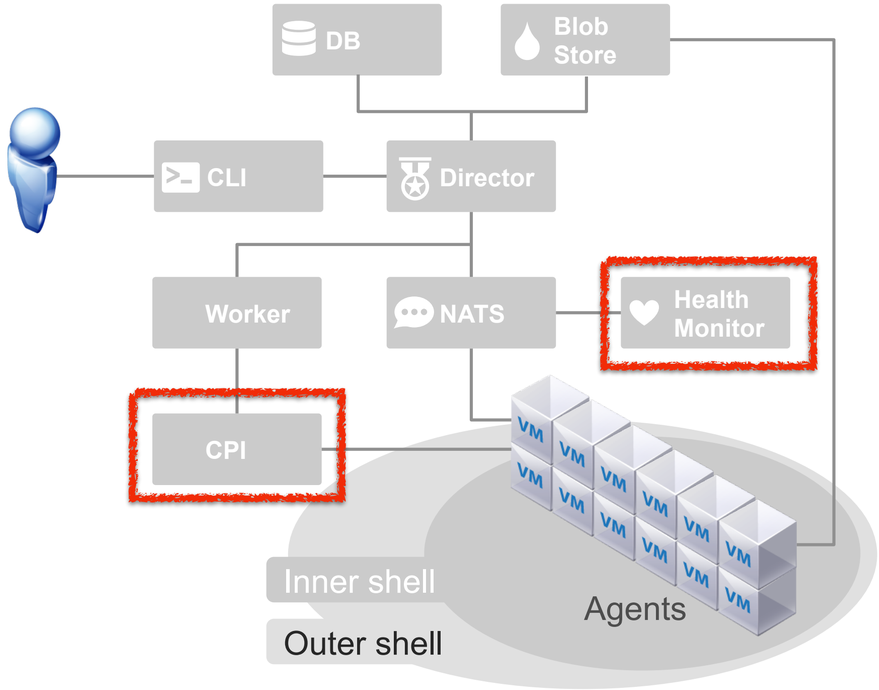
The **Health Monitor** provides lifecycle availability for all deployed VM's and VM processes.

The **Cloud Provider Interface** (CPI) abstracts the underlying IaaS provider, allowing bosh deployed clusters to operate on any IaaS which has a CPI.

Ops Manager & BOSH

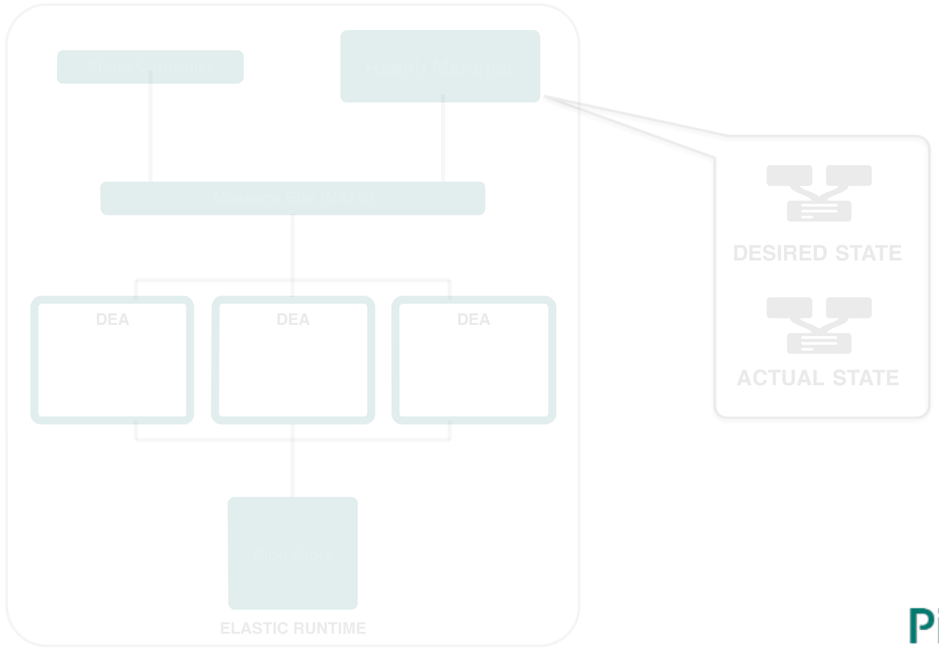
vmware amazon web services Windows Azure Google Cloud Platform openstack

BOSH deploys and manages large scale distributed systems. It provides the means to go from deployment (i.e., Chef/Puppet) to VM creation and lifecycle management. Core to bosh is the ability to execute **Canary-style deployments** with zero downtime.



Pivotal

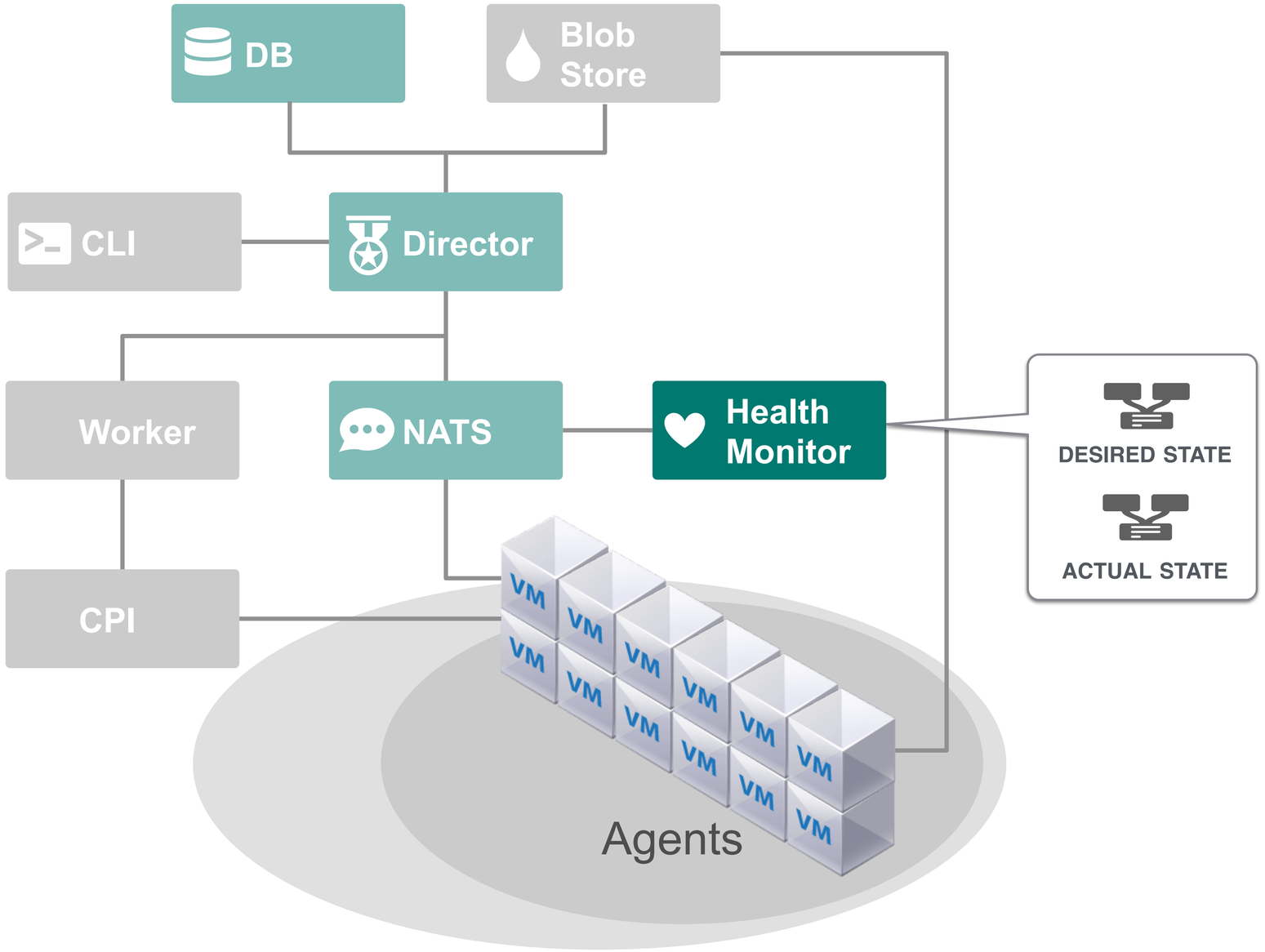
4 Levels of High Availability



Pivotal

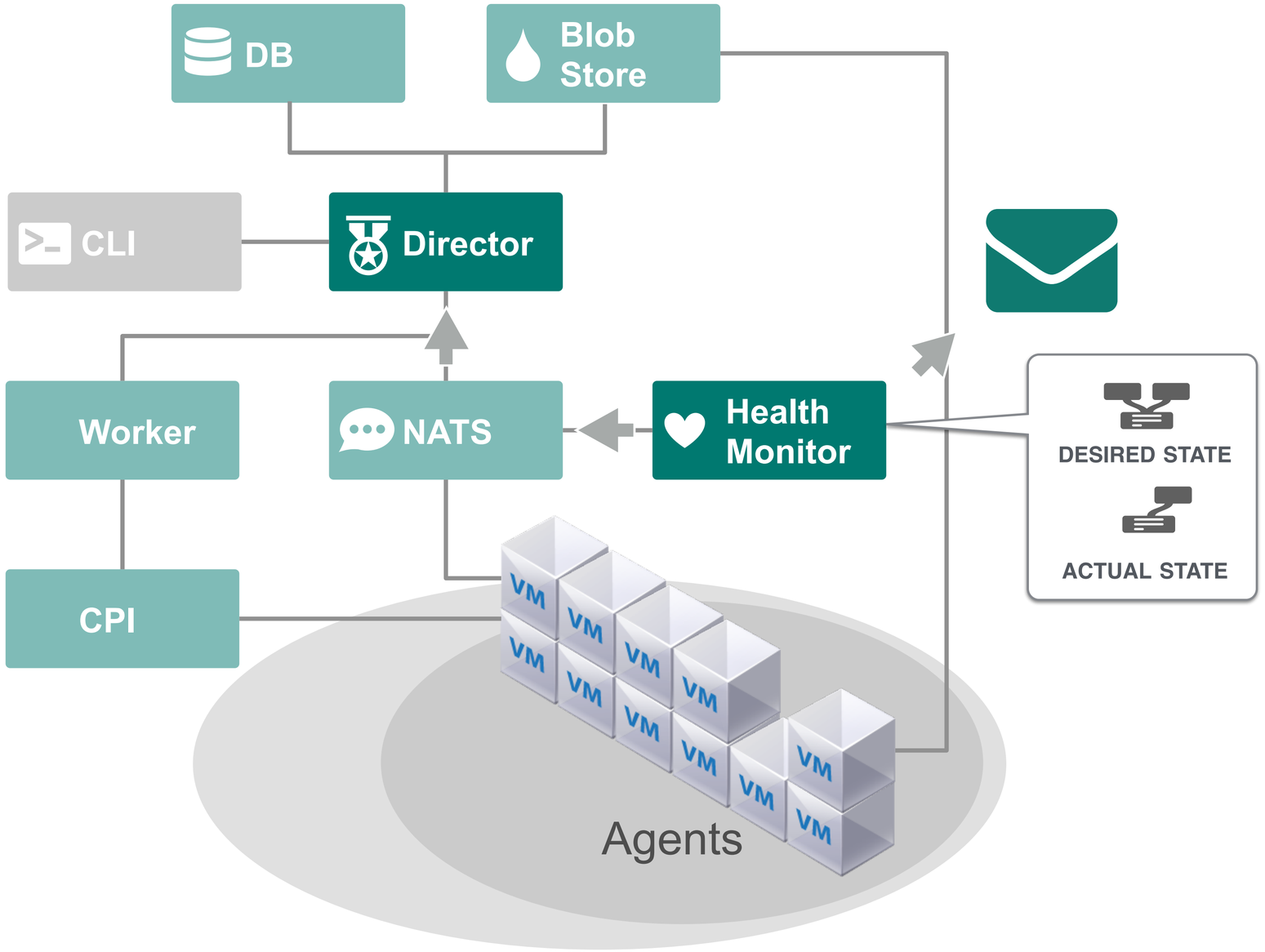
Failed VMs are Recovered

4 Levels of High Availability



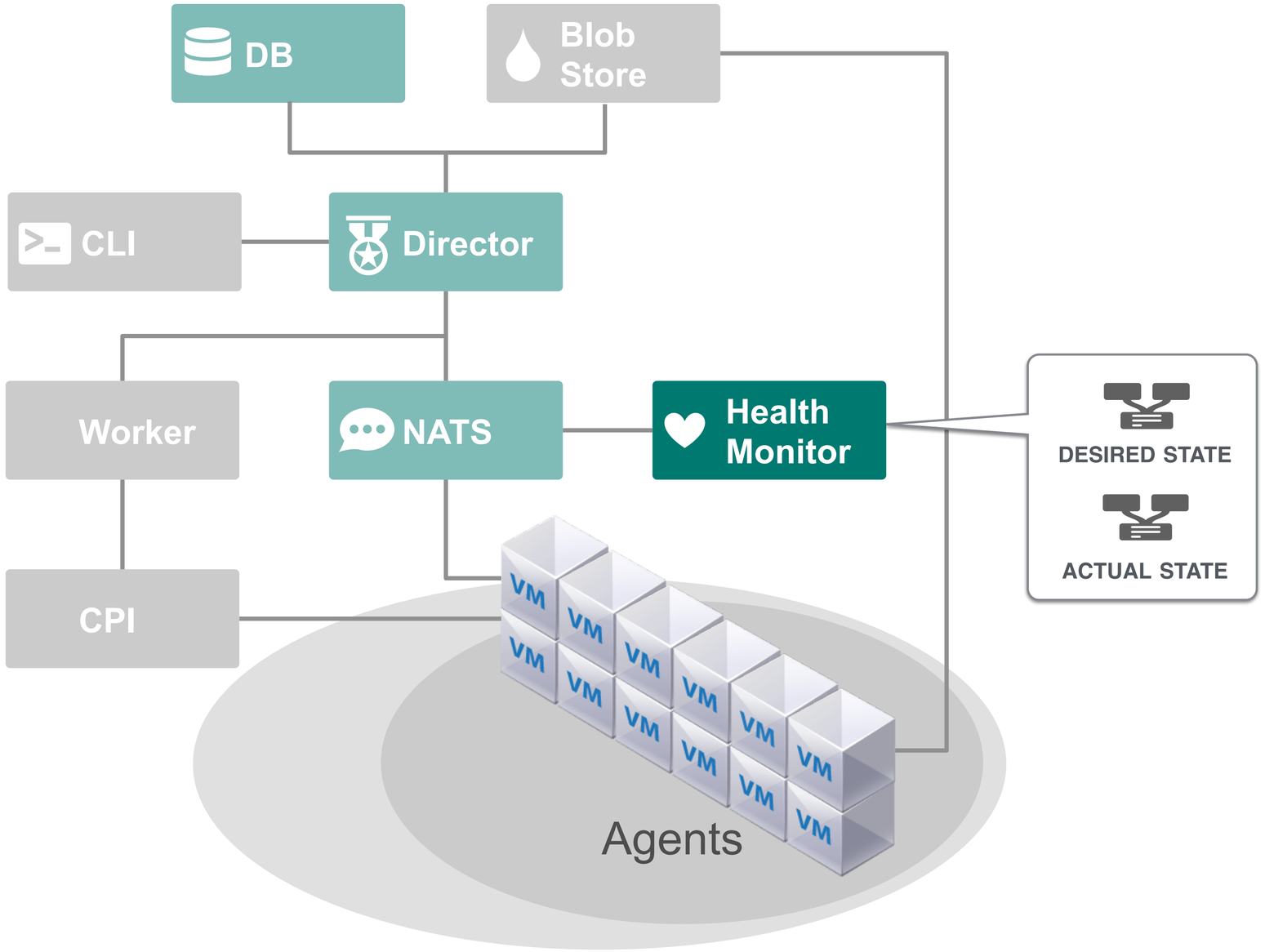
Failed VMs are Recovered

4 Levels of High Availability

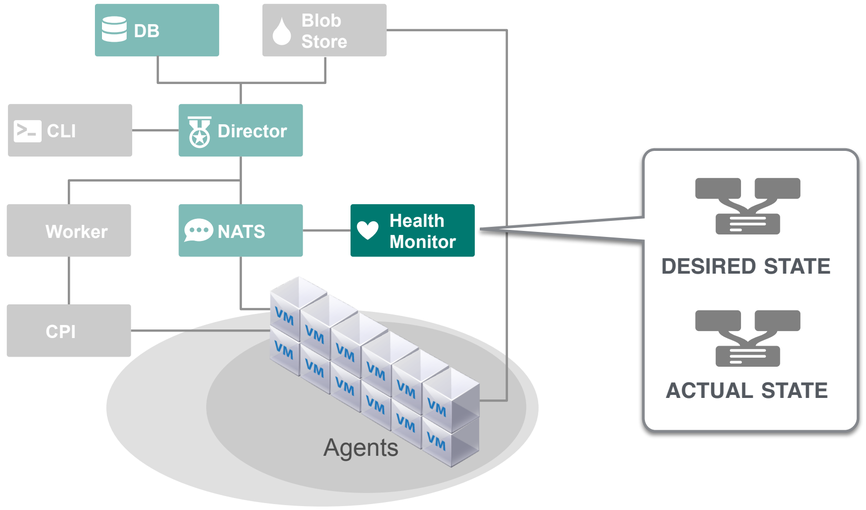


Failed VMs are Recovered

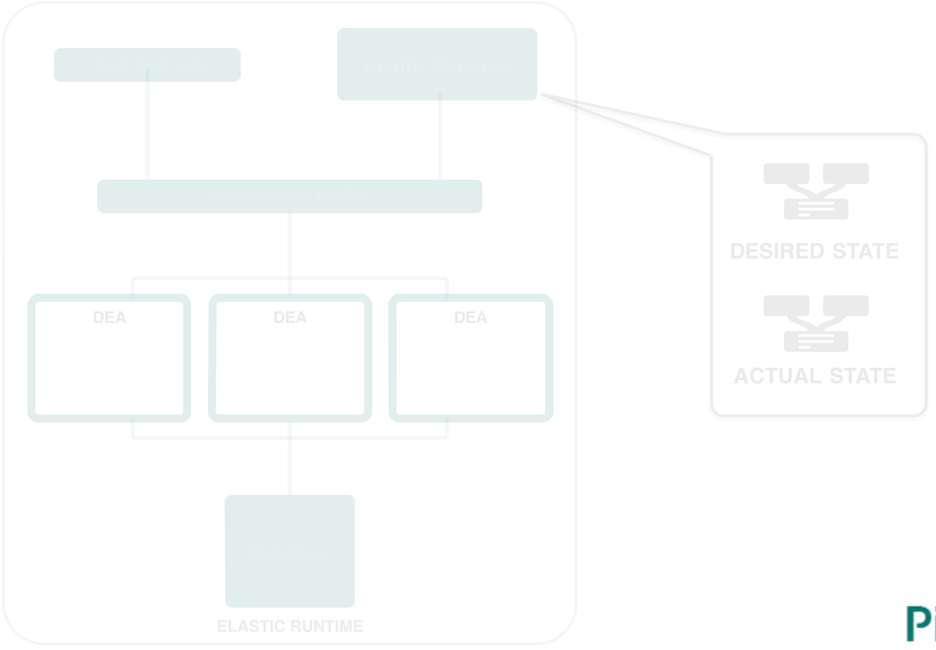
4 Levels of High Availability



4 Levels of High Availability



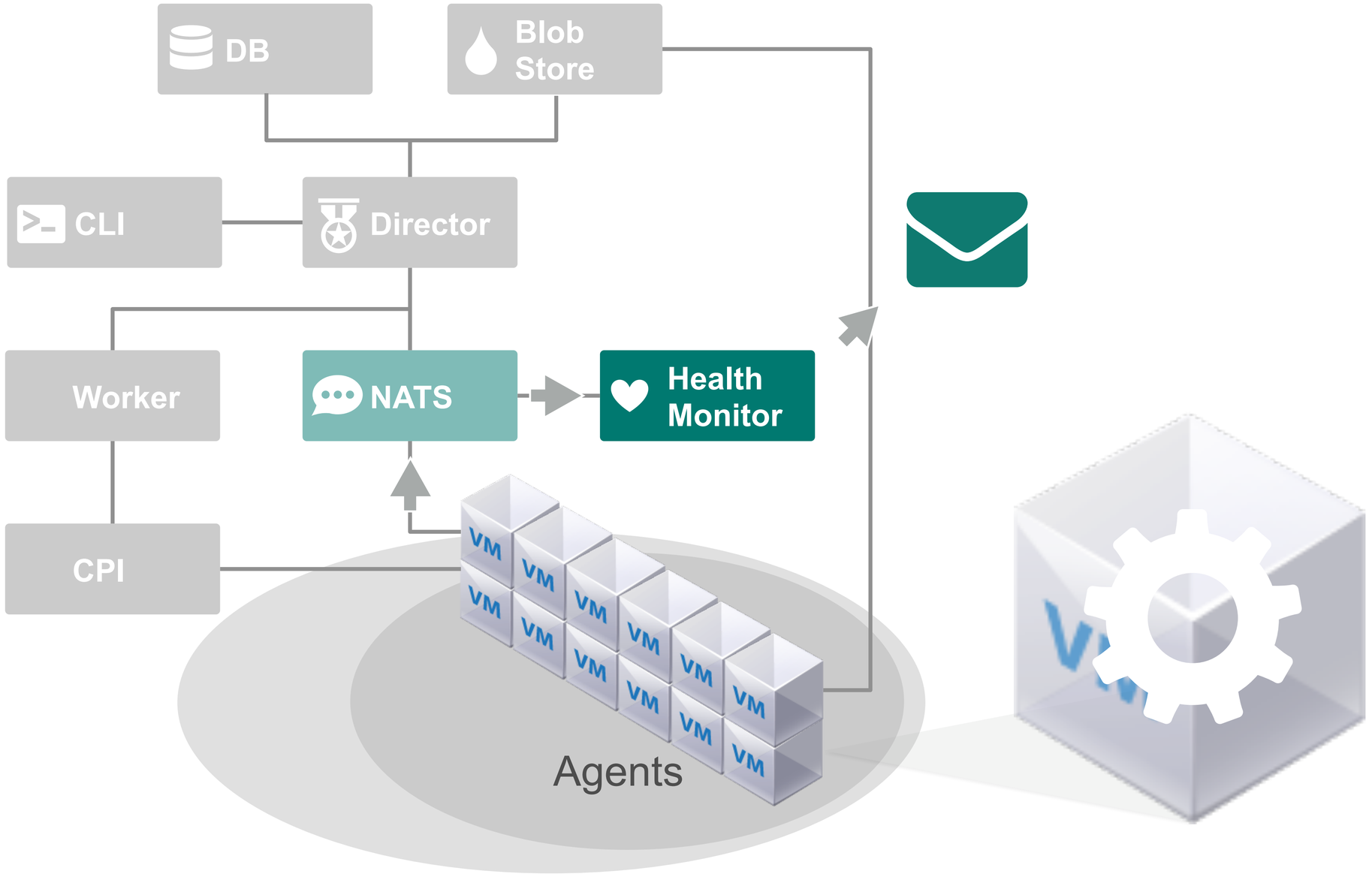
Failed VMs are Recovered



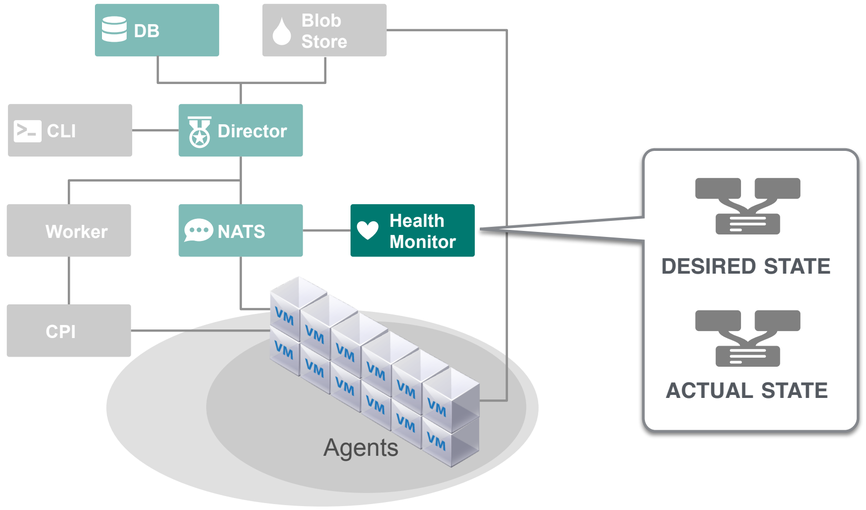
Pivotal

Failed Processes are Recovered

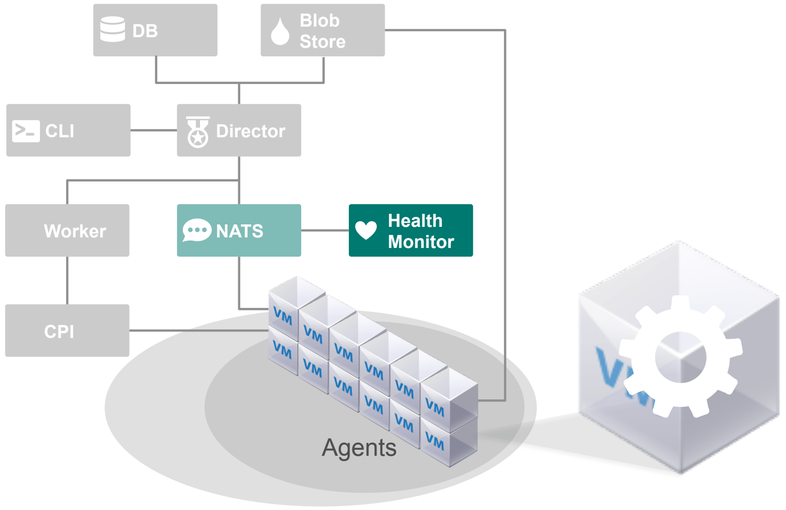
4 Levels of High Availability



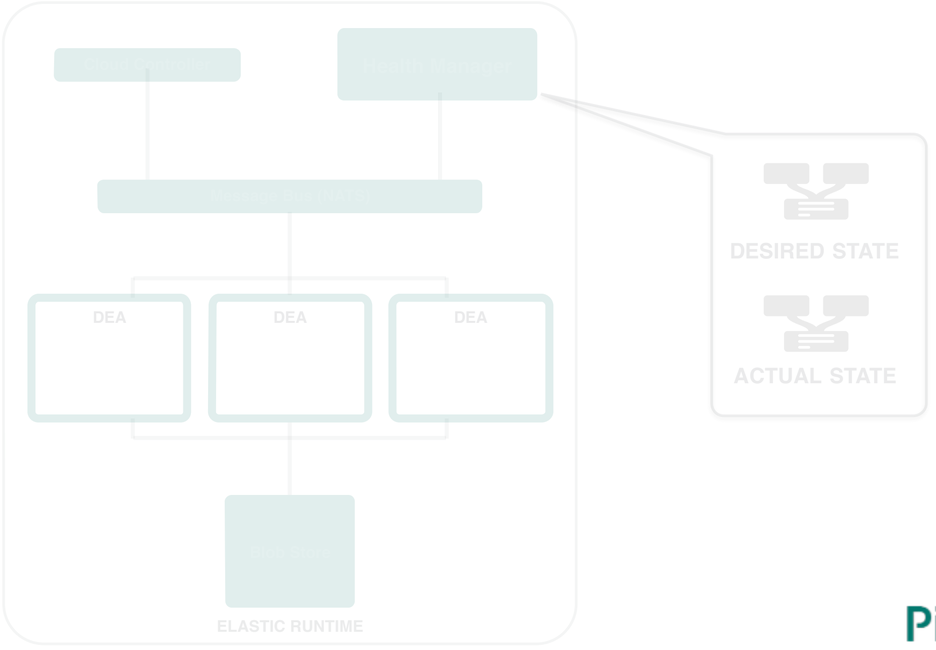
4 Levels of High Availability



Failed VMs are Recovered



Failed Processes are Recovered



Pivotal

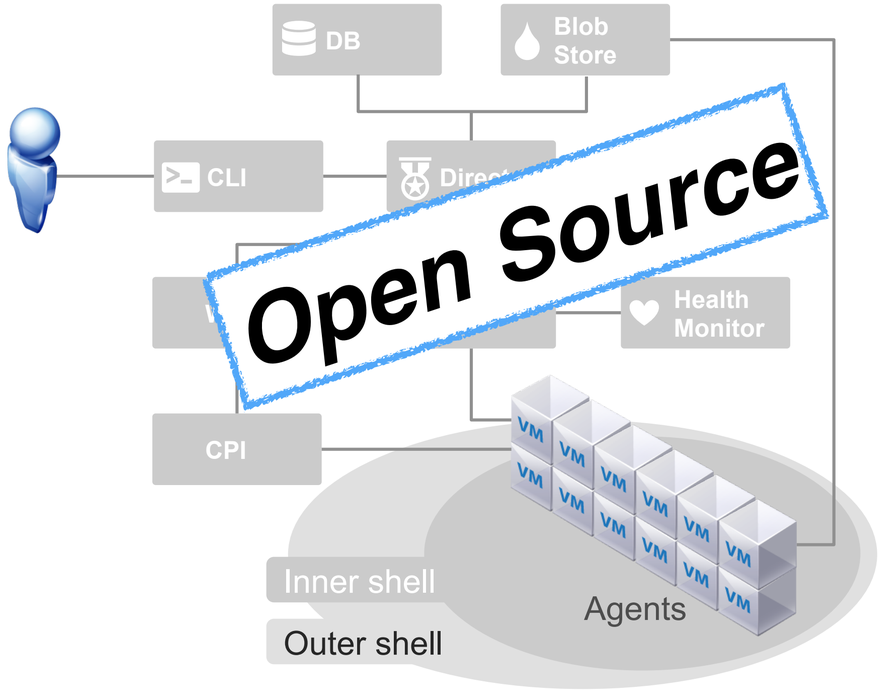
The **Health Monitor** provides lifecycle availability for all deployed VM's and VM processes.

The **Cloud Provider Interface** (CPI) abstracts the underlying IaaS provider, allowing bosh deployed clusters to operate on any IaaS which has a CPI.

Ops Manager & BOSH

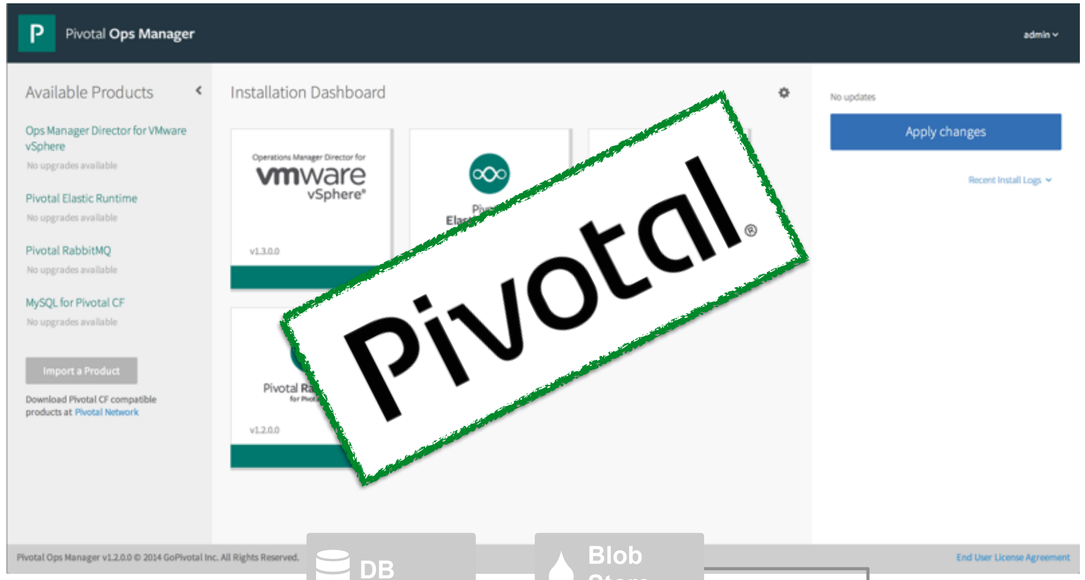
vmware amazon web services Windows Azure Google Cloud Platform openstack

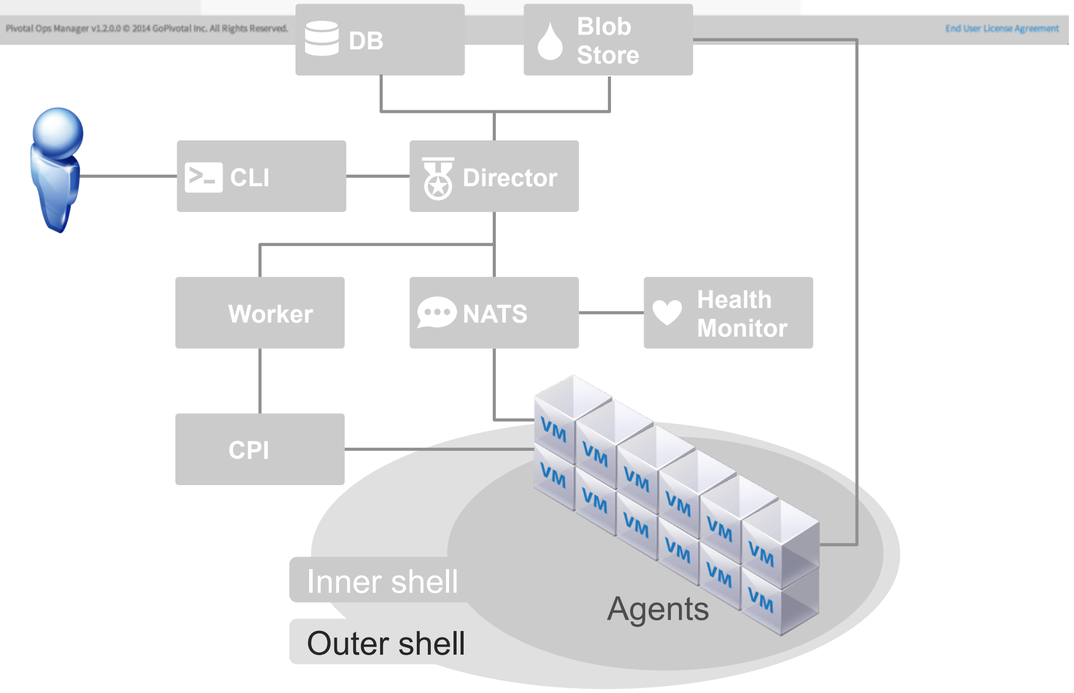
BOSH deploys and manages large scale distributed systems. It provides the means to go from deployment (i.e., Chef/Puppet) to VM creation and lifecycle management. Core to bosh is the ability to execute **Canary-style deployments** with zero downtime.



Pivotal

Ops Manager is a web based front end to manage Pivotal CF installations and associated services. Ops Manager leverages BOSH to deploy and manage clusters.





Ops Manager & BOSH

vmware
amazon web services
Windows Azure
Google Cloud Platform
openstack

Pivotal

HA Proxy

Message Bus (NATS)

MESSAGING

Ops Manager & BOSH

vmware amazon web services Windows Azure Google Cloud Platform openstack

All Cloud Foundry traffic flows through a **proxy server**. CF can be fronted by the packaged HAProxy or a customer provided proxy. The proxy server is responsible for SSL termination.

NATS is a *fast* internal messaging bus that provides **system wide communication** via a publish-and-subscribe mechanism.

Pivotal

HA Proxy

Open Source

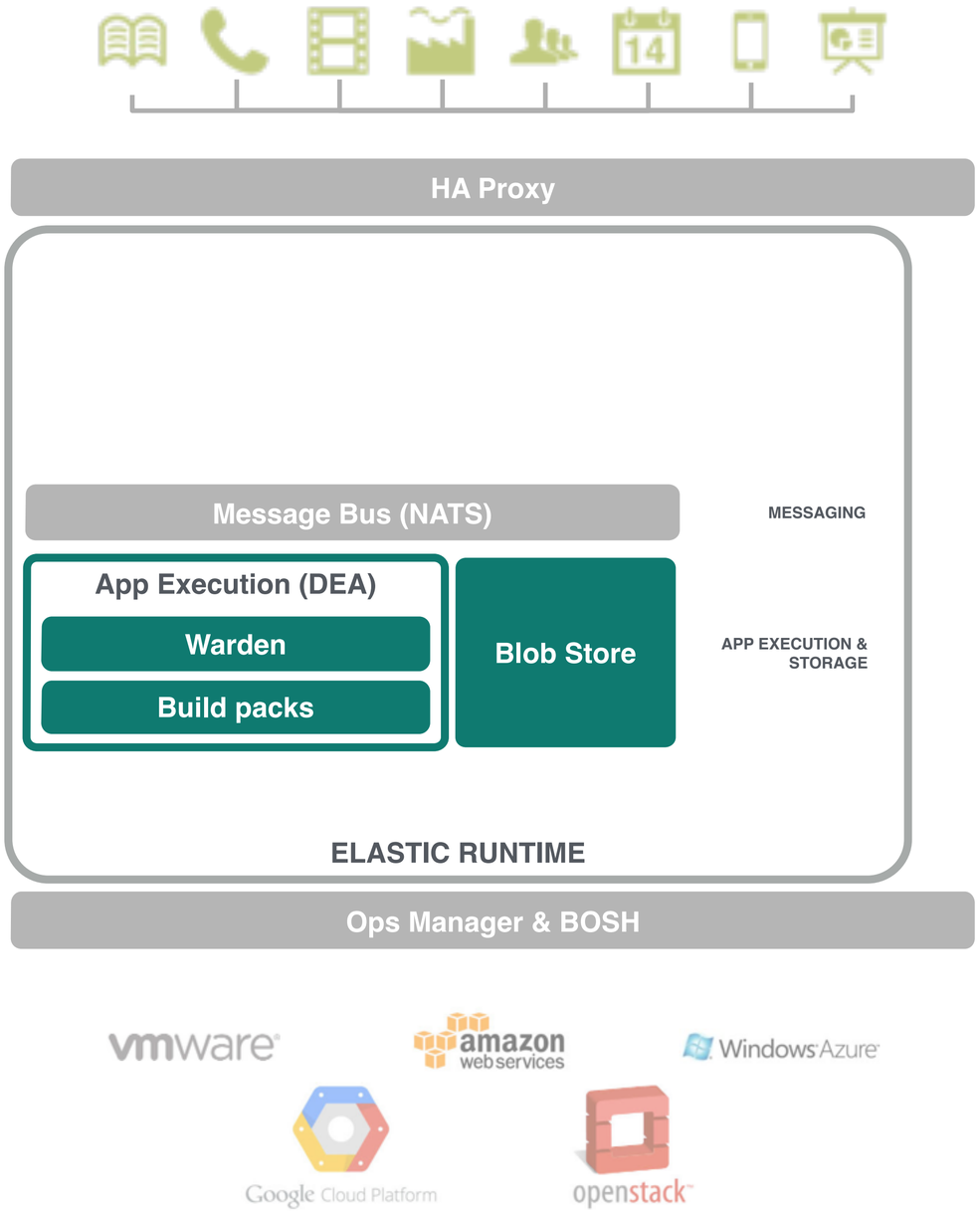
ELASTIC RUNTIME

Ops Manager & BOSH

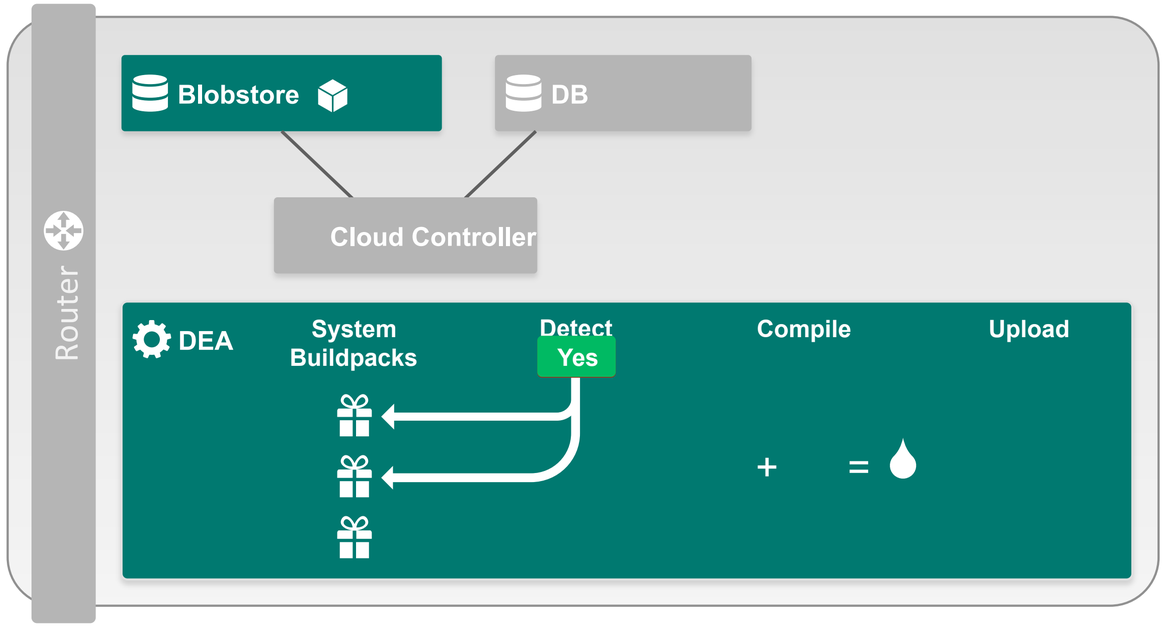
vmware amazon web services Windows Azure Google Cloud Platform openstack

The **Elastic Runtime *is* Cloud Foundry**. It is made up a of a set of micro services that provide a comprehensive PaaS platform.

Pivotal



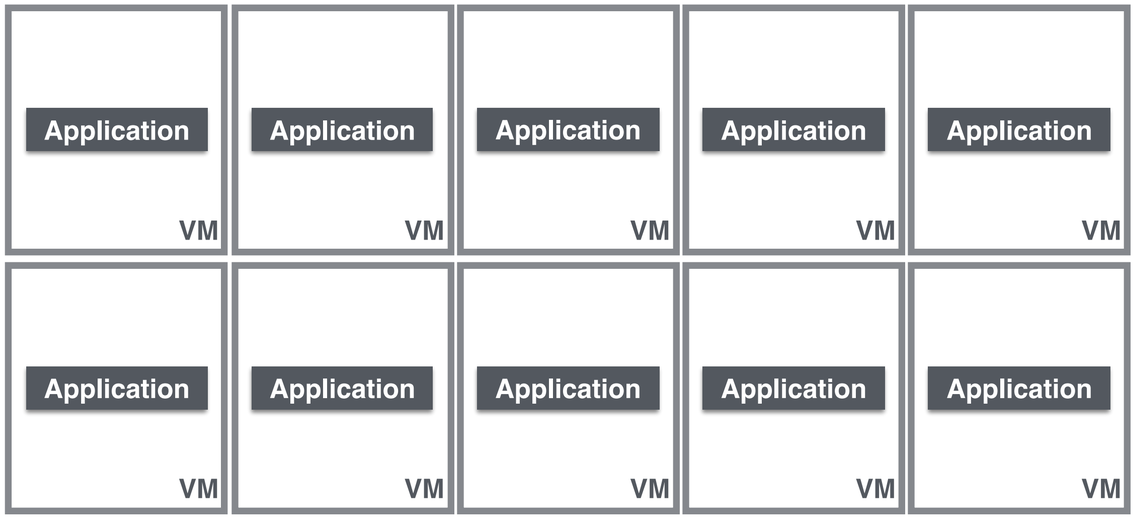
Application instances run inside of **Warden** containers, using a **Build Pack** for the runtime, on **Droplet Execution Agent** (DEA) virtual machines. Application code + Build pack = a Droplet, which is cached in the **Blob Store**.



Pivotal

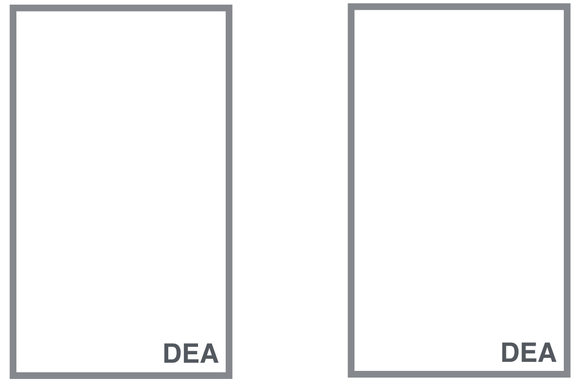
Application Density

APP EXECUTION & STORAGE



amazon web services

More Application Instances
… **Less** Resources!

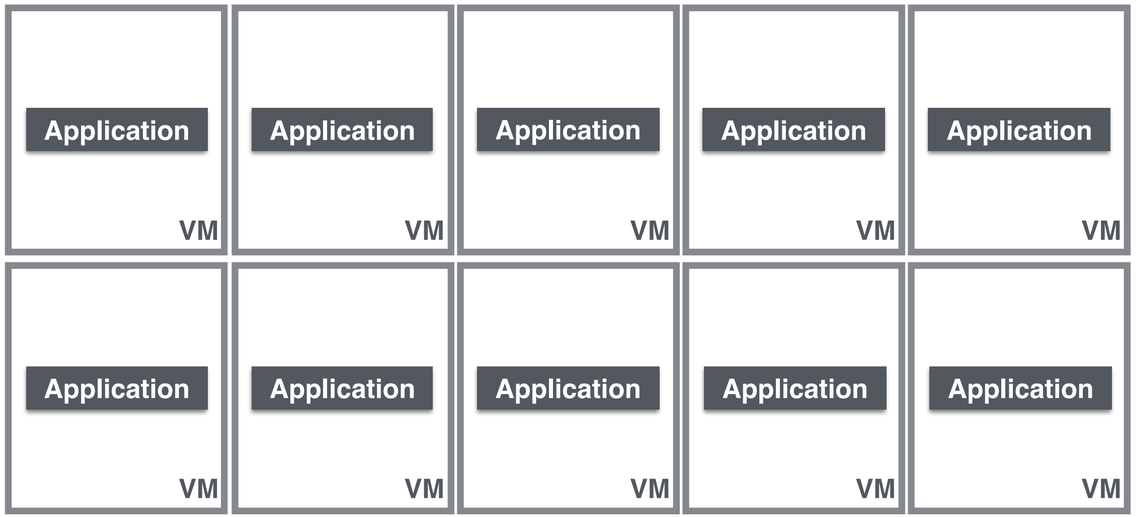


CLOUD FOUNDRY™

Pivotal

SCALE/RECOVERY SPEED

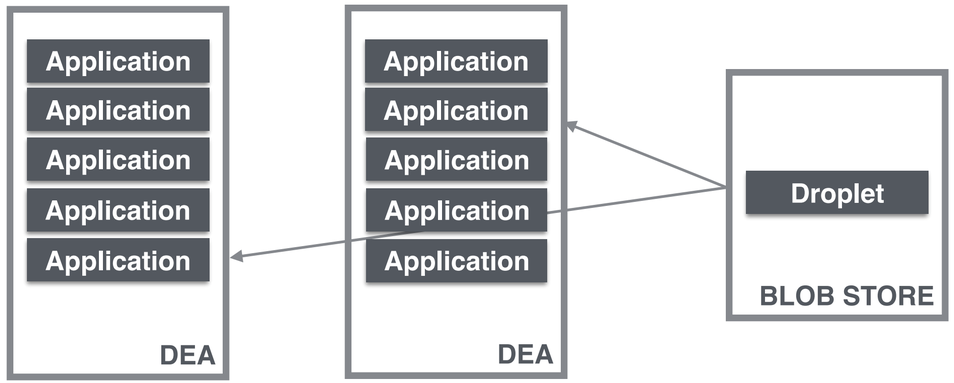
APP EXECUTION & STORAGE



2-5 minutes

amazon web services

Faster scaling…
faster recovery!



CLOUD FOUNDRY™

< 10 seconds

Pivotal

BUILD PACKS

App Execution (DEA)

Warden

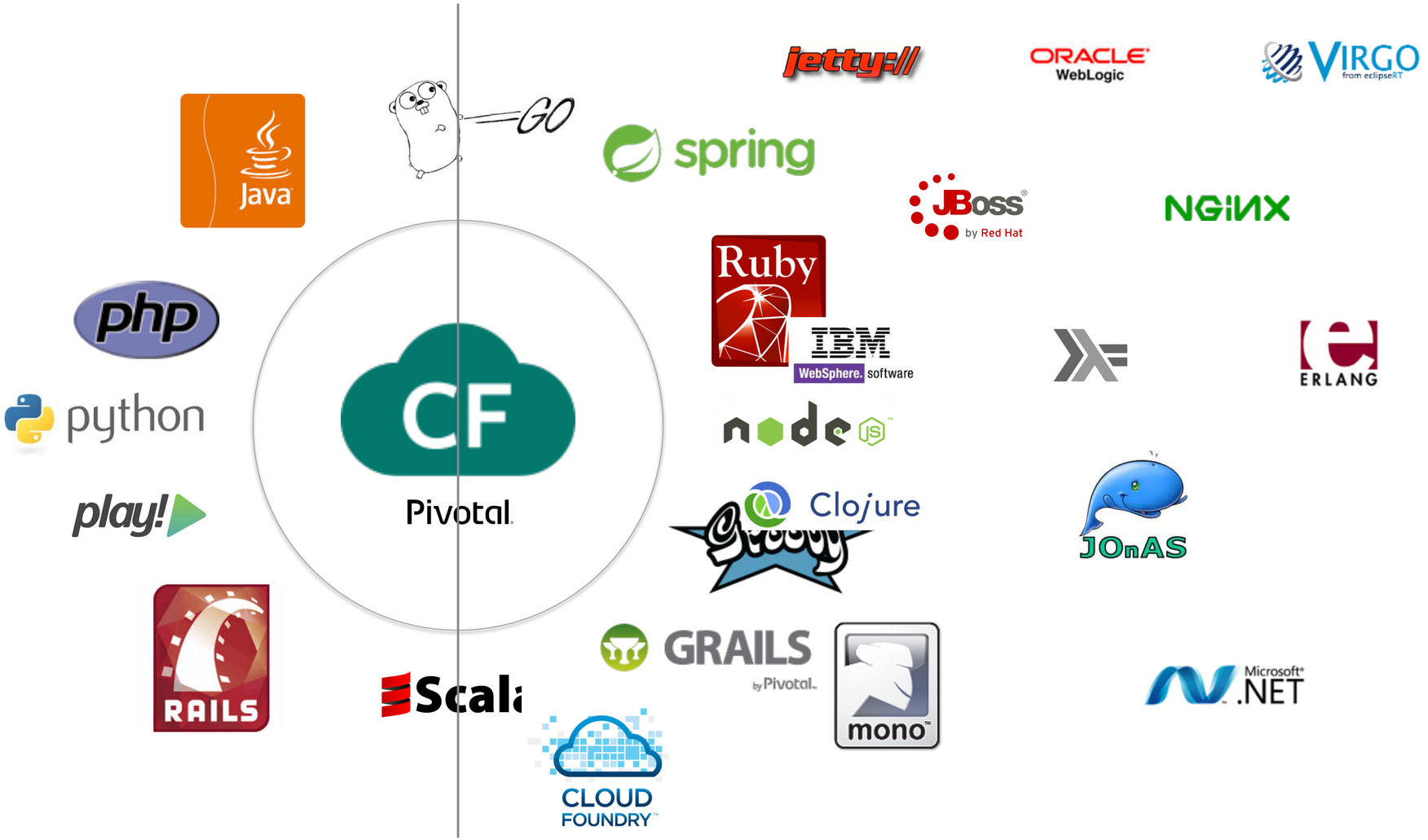
Build packs

Blob Store

APP EXECUTION & STORAGE

Build Packs

APP EXECUTION & STORAGE



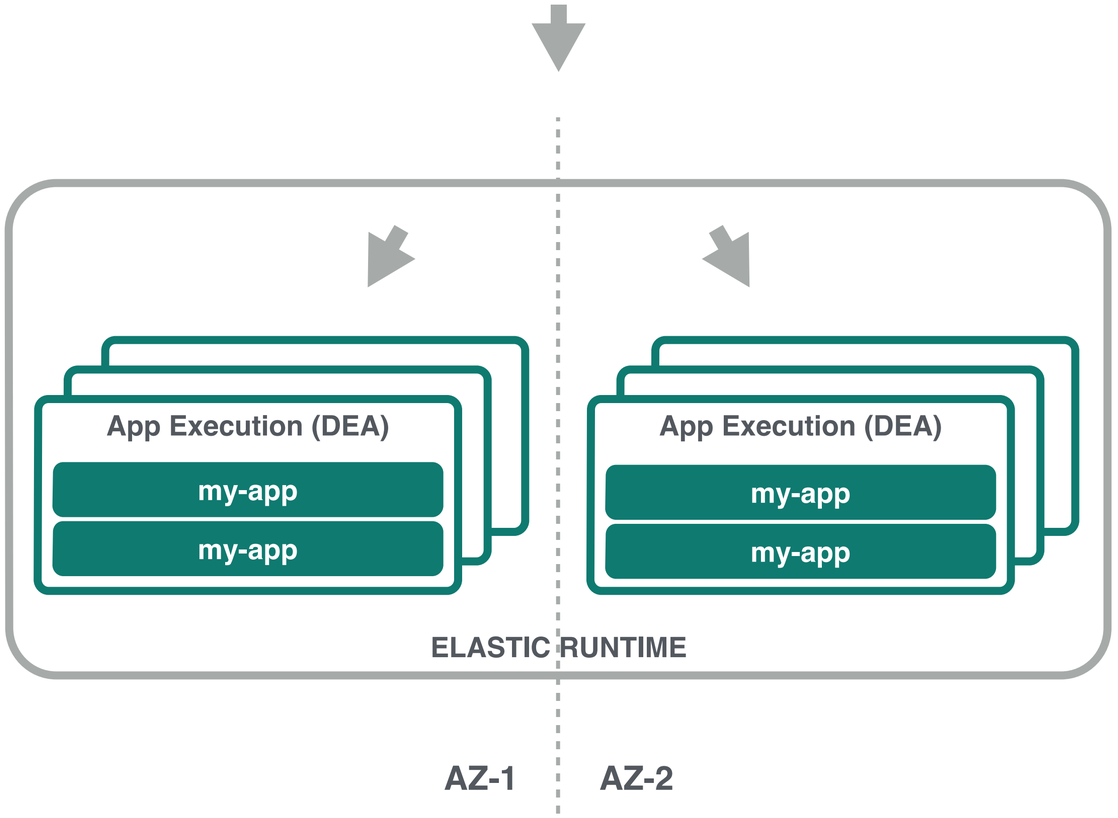
Only Pivotal CF Operates Offline

Pivotal

Application Instances Balanced across Availability Zones

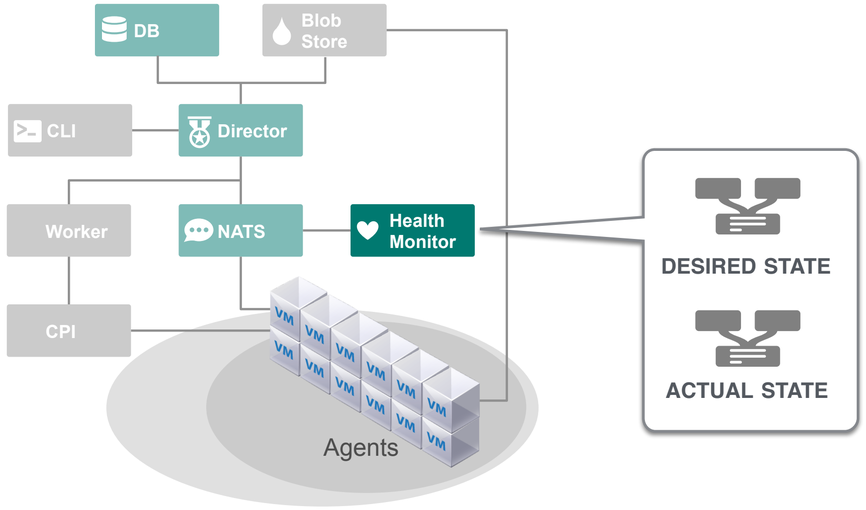
4 Levels of High Availability

cf push my-app -i 4

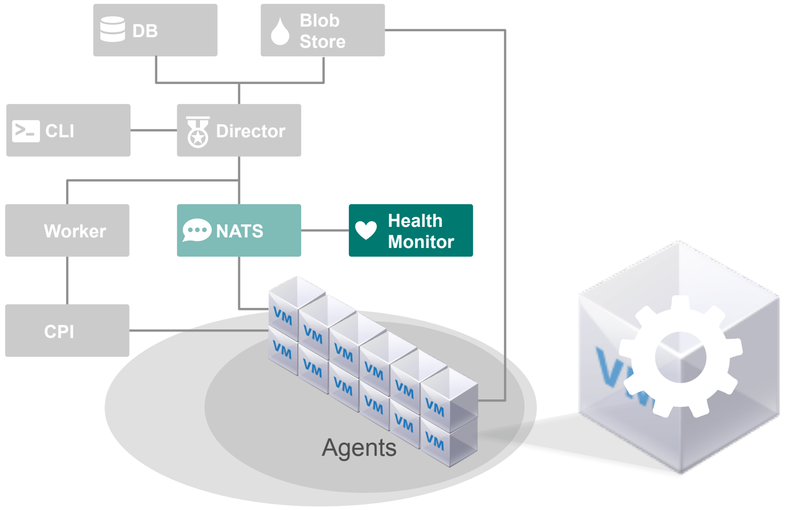


Pivotal

4 Levels of High Availability

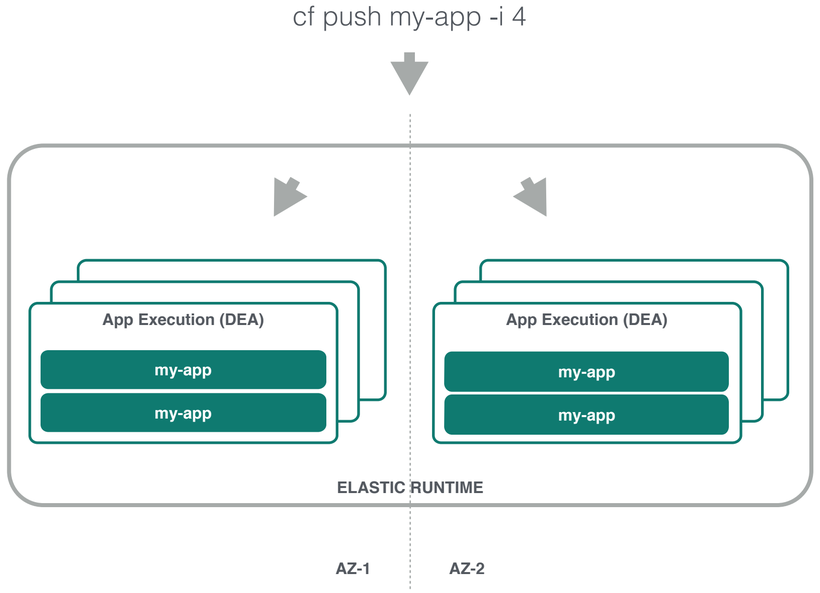


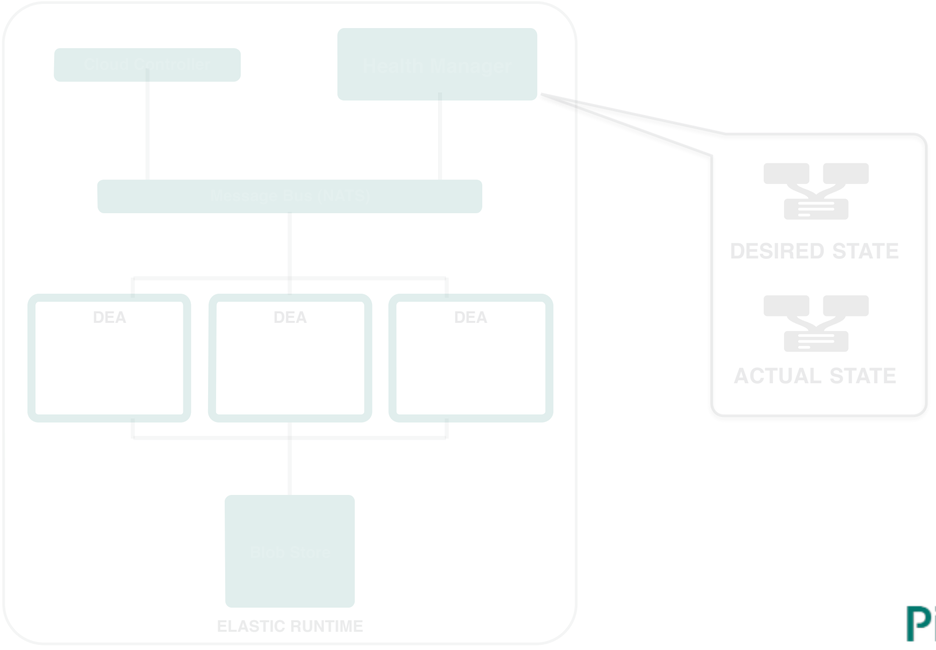
Failed VMs are Recovered



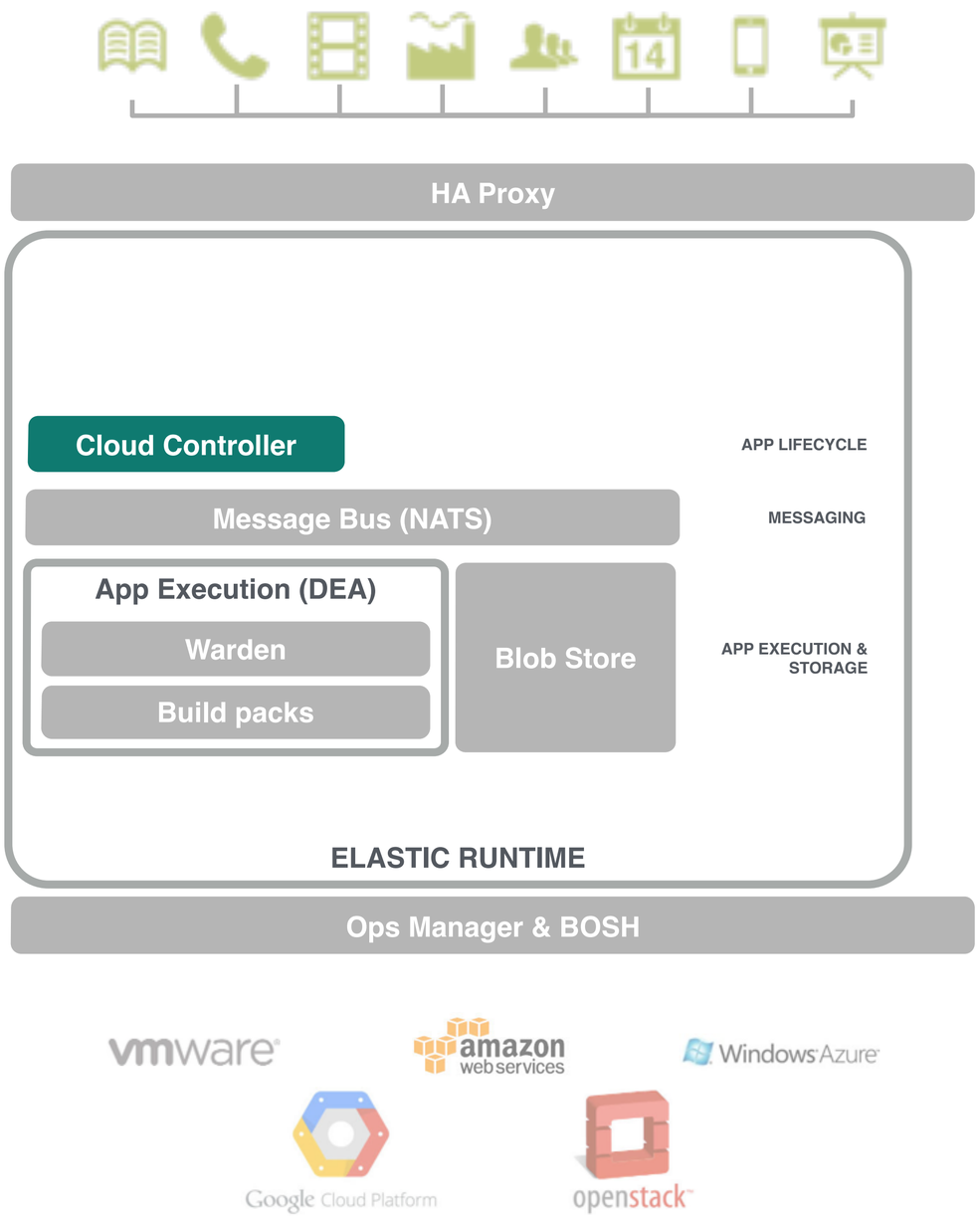
Failed Processes are Recovered

Application Instances Balanced across Availability Zones

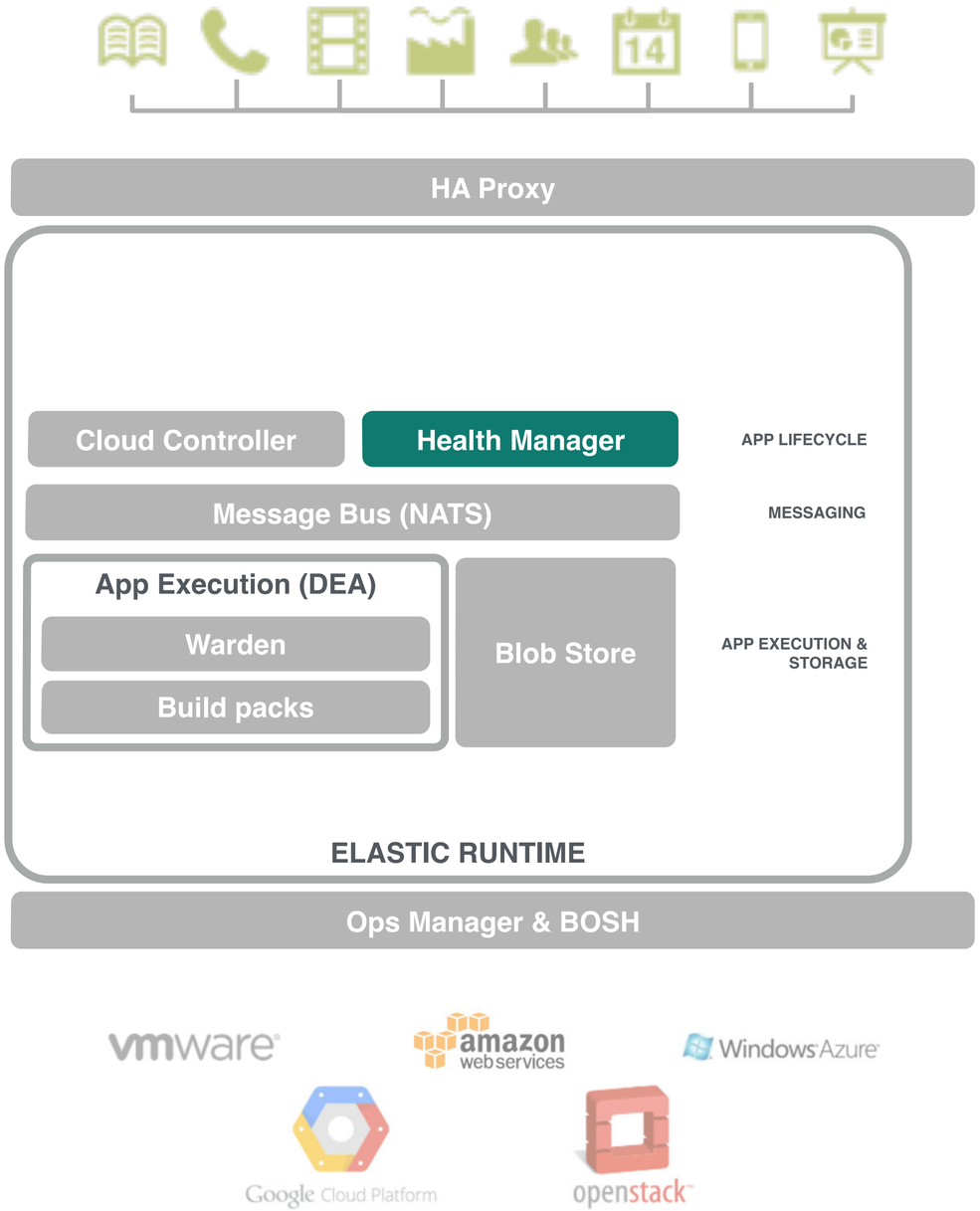




Pivotal



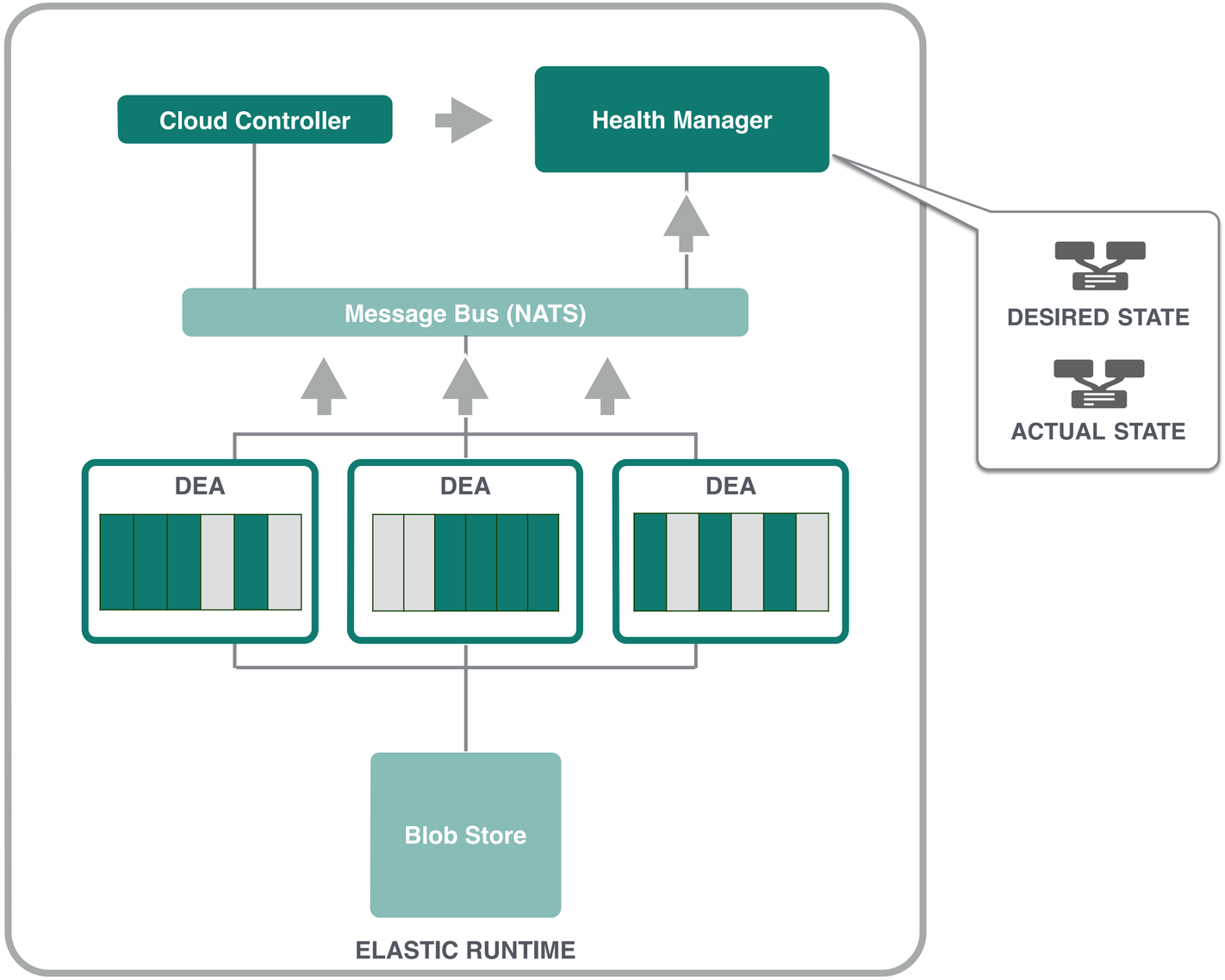
The **Cloud Controller** handles all client requests including pushing applications. It is responsible for expected app state, state transitions, and desired convergence.



The **Health Manager** monitors application uptime by listening to the NATS message bus for mismatched application states (expected vs. actual). The Cloud Controller publishes expected state and the DEAs publish actual state. State mismatches are reported to the Cloud Controller.

Failed Application Instances are Recovered

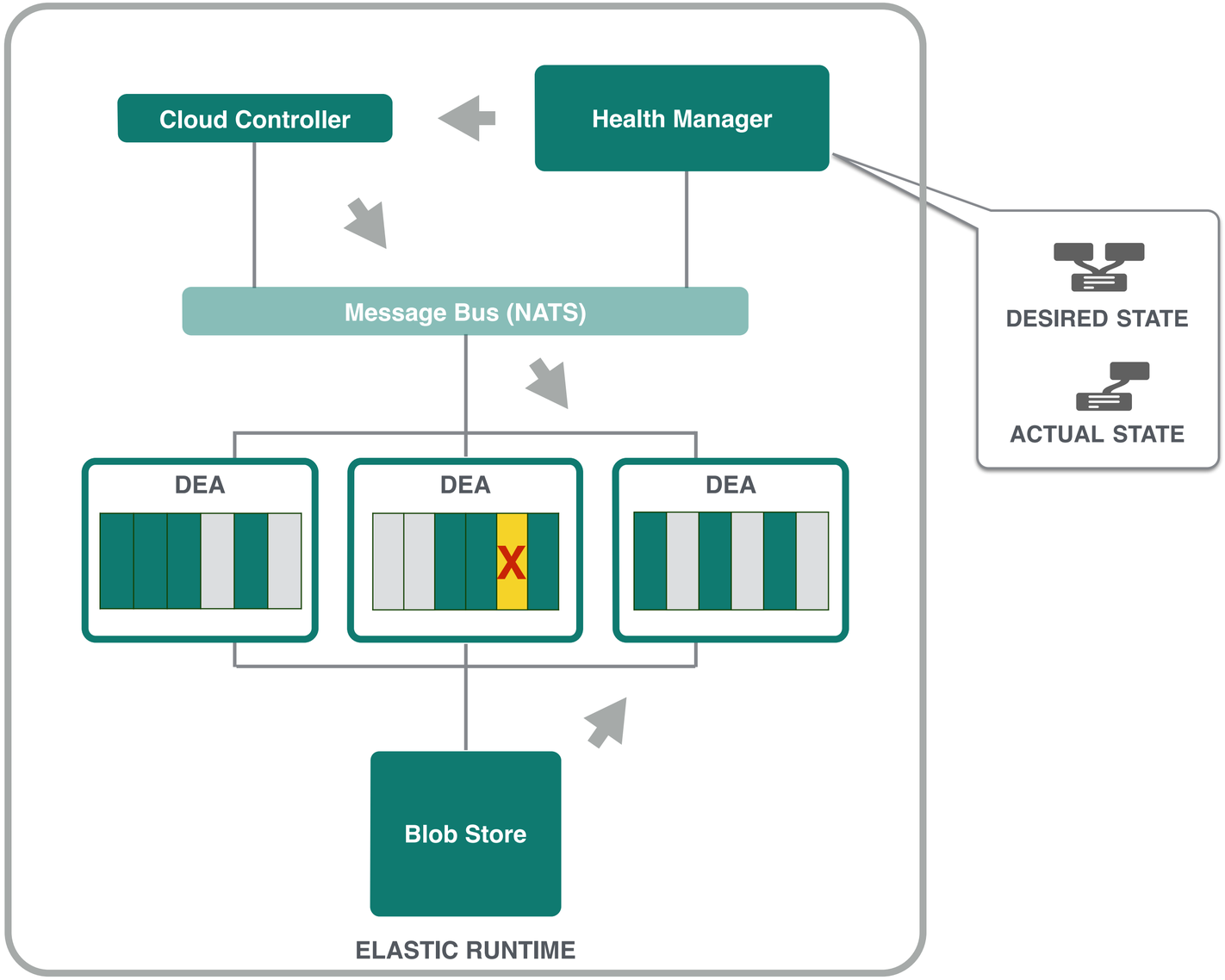
4 Levels of High Availability



Pivotal

Failed Application Instances are Recovered

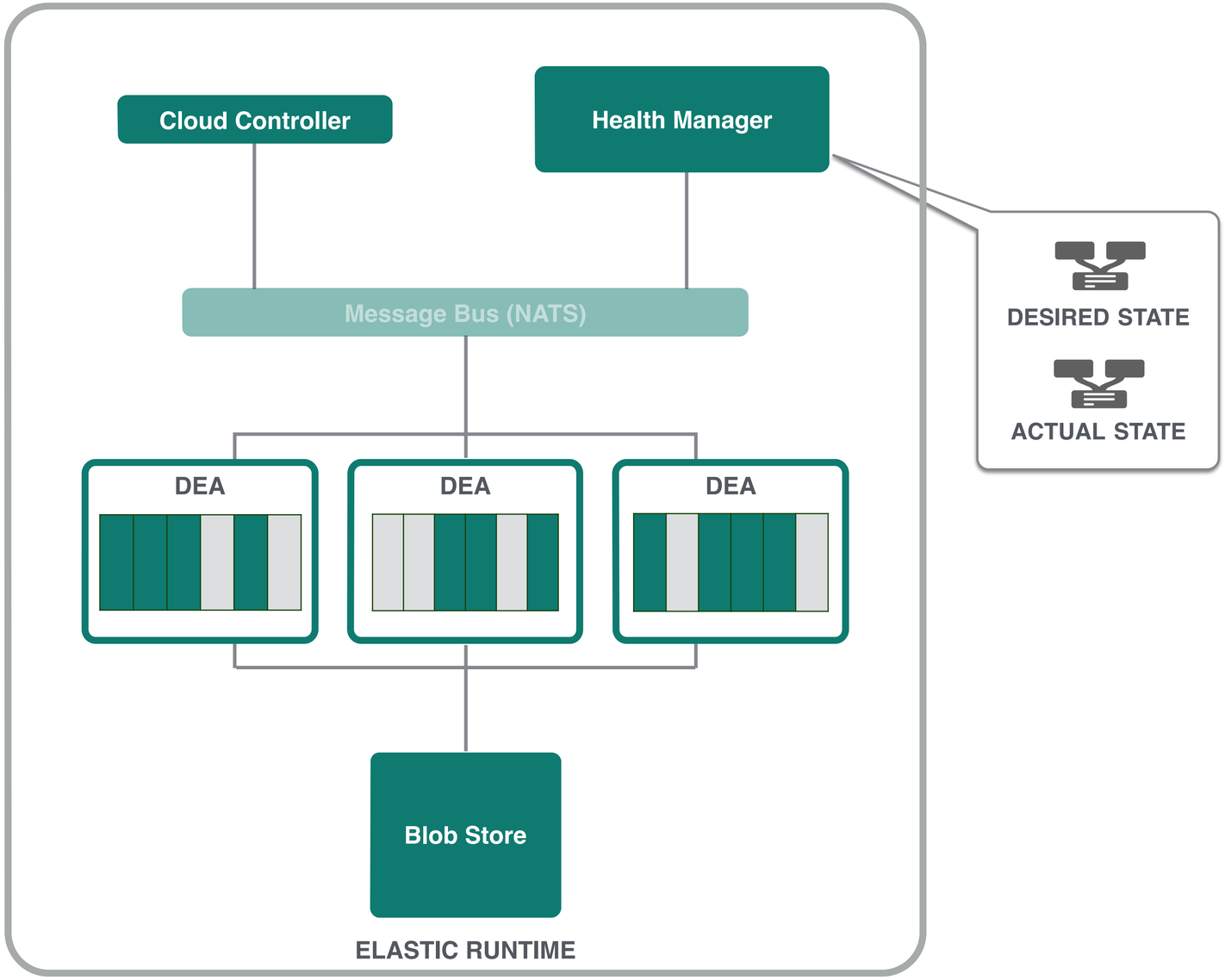
4 Levels of High Availability



Pivotal

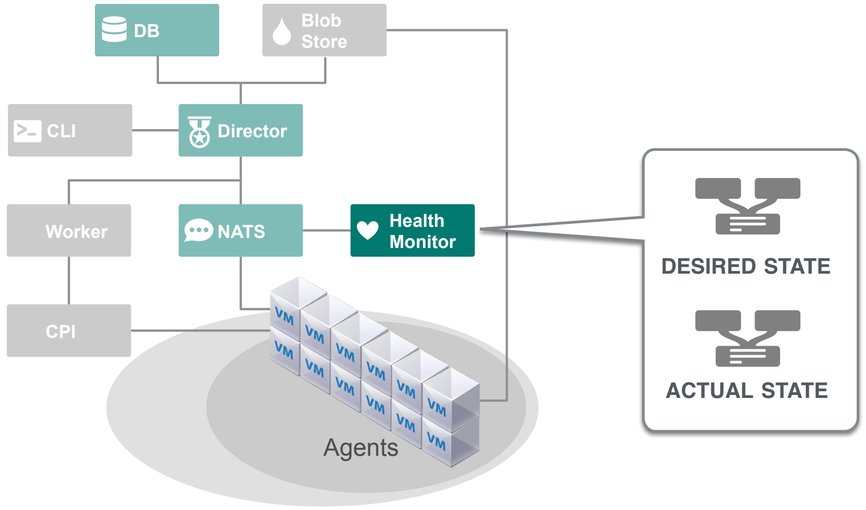
Failed Application Instances are Recovered

4 Levels of High Availability

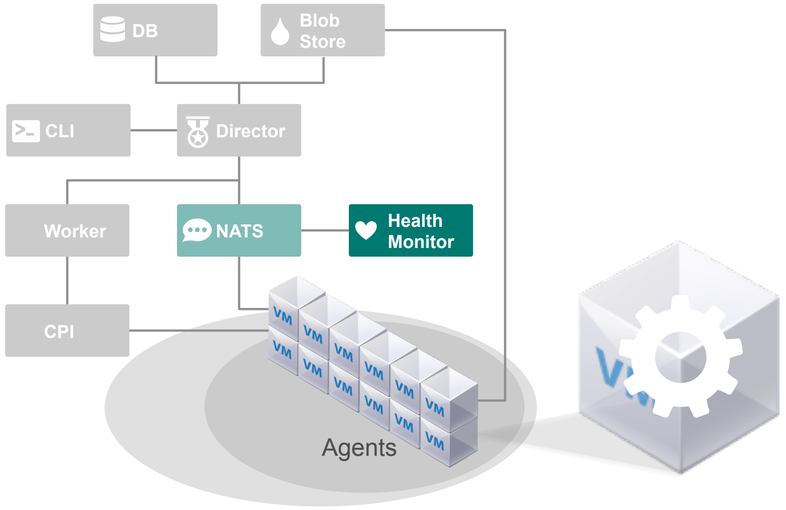


Pivotal

4 Levels of High Availability

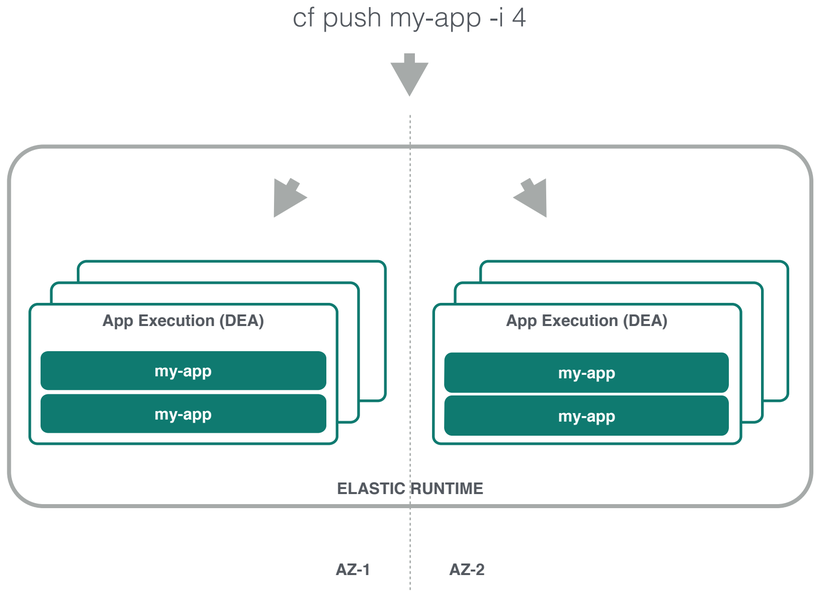


Failed VMs are Recovered

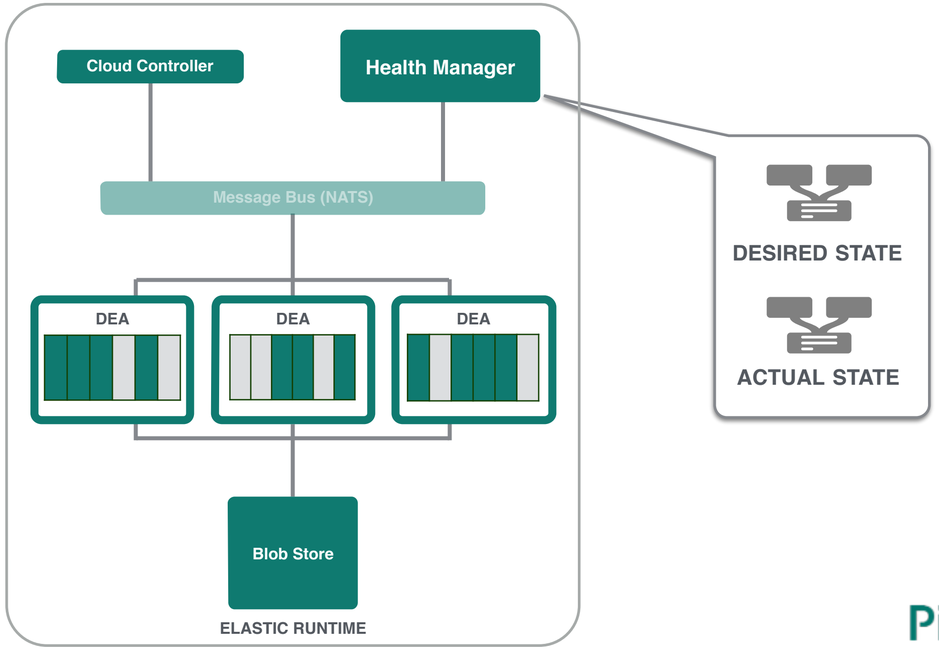


Failed Processes are Recovered

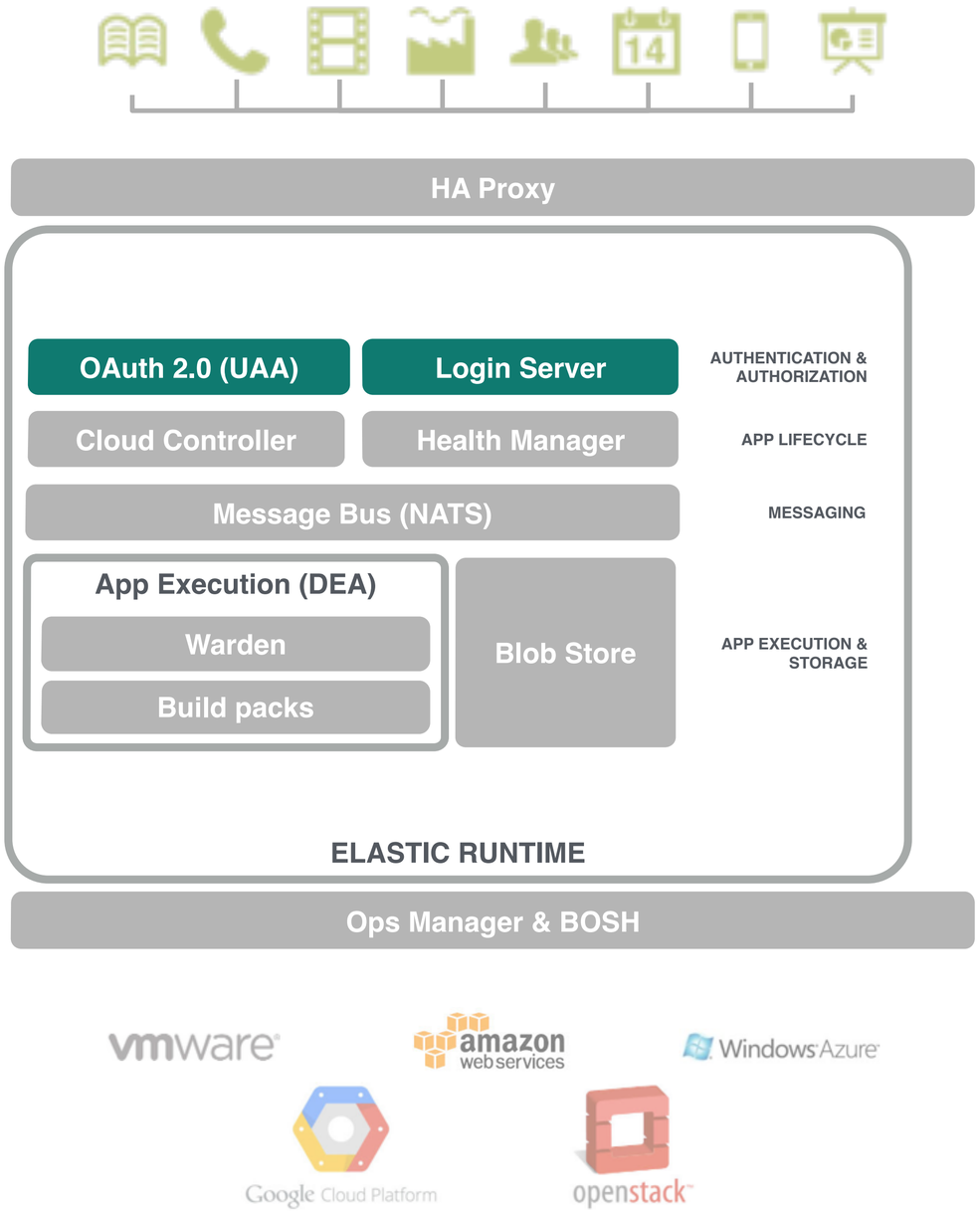
Application Instances Balanced across Availability Zones



Failed Application Instances are Recovered

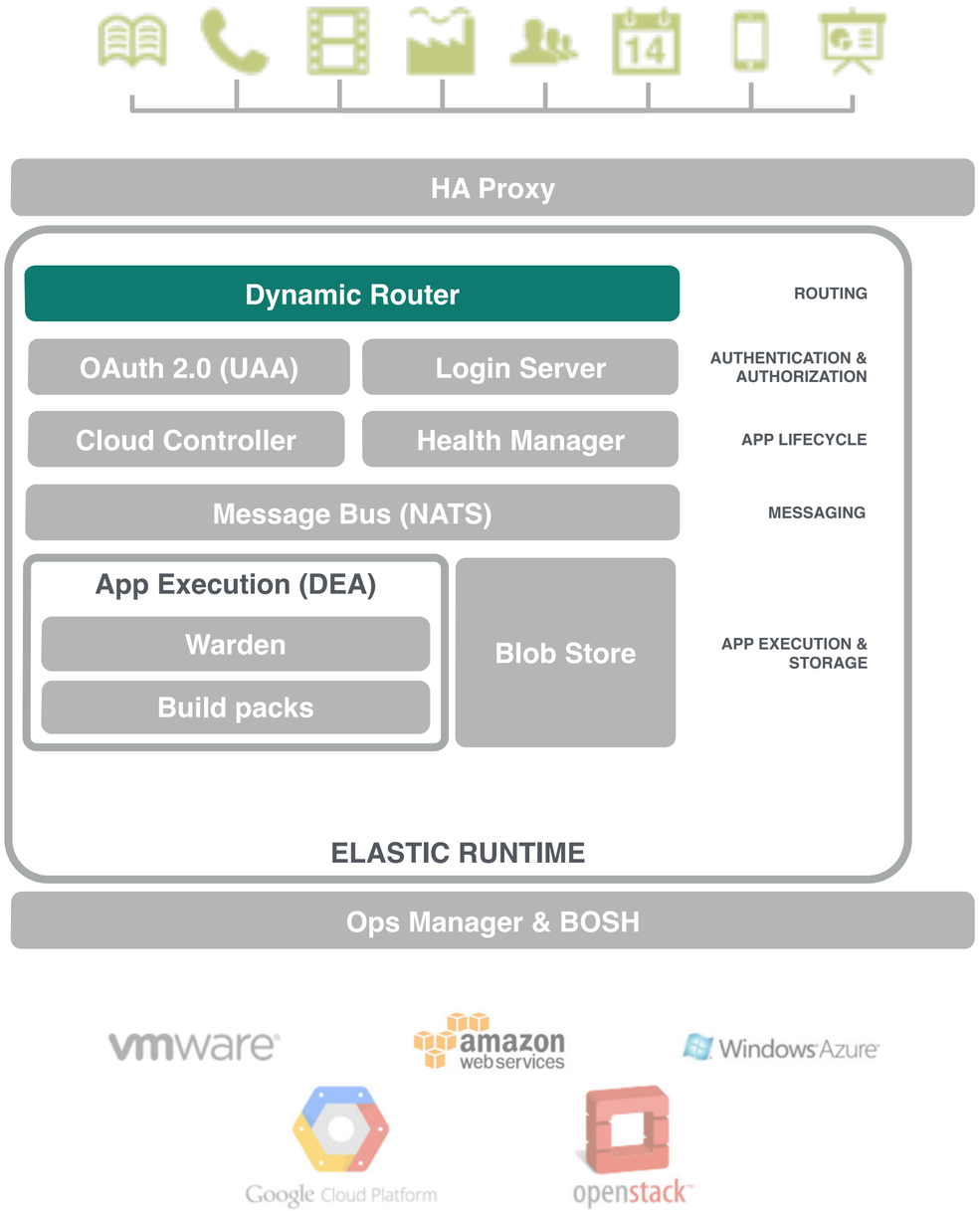


Pivotal



User Authorization and Authentication provides identity, security and authorization services. It manages third party Oauth 2.0 access credentials and can provide application access and identity-as-a-service for apps running on Cloud Foundry.

The **Login Server** can leverage external LDAP sources, including Active Directory, for authentication.



The **router** shapes and routes all external system traffic (HTTP/API) and application traffic from the internet/intranet. It maintains a dynamic routing table for each load-balanced app instance with IP addresses and ports.

BLUE/GREEN DEPLOYMENTS

HA Proxy

Dynamic Router

OAuth 2.0 (UAA)

Login Server

Cloud Controller

Health Manager

Message Bus (NATS)

App Execution (DEA)

Warden

Build packs

Blob Store

ROUTING

AUTHENTICATION & AUTHORIZATION

APP LIFECYCLE

MESSAGING

APP EXECUTION & STORAGE

ELASTIC RUNTIME

Ops Manager & BOSH

vmware

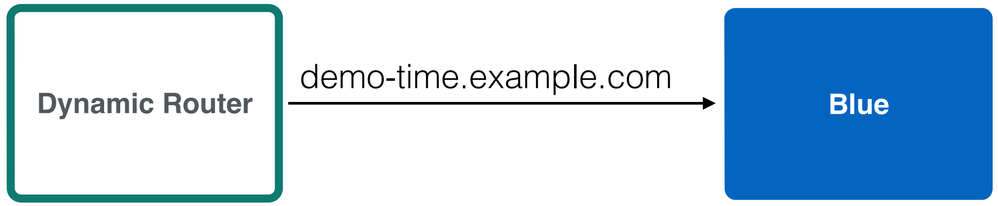
amazon web services

Windows Azure

Google Cloud Platform

openstack

cf push Blue -n demo-time



Pivotal

BLUE/GREEN DEPLOYMENTS

HA Proxy

ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

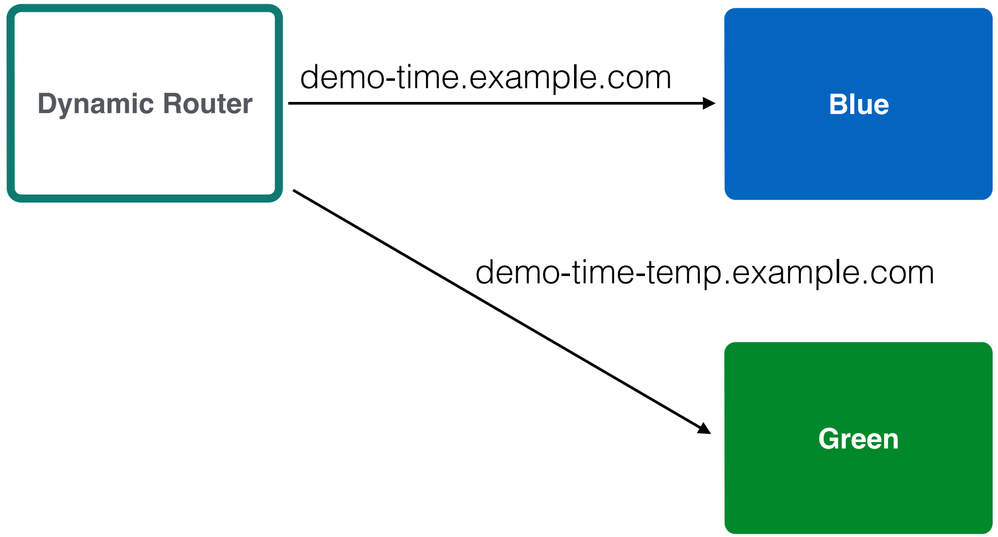
App Execution (DEA): Warden, Build packs | Blob Store — APP EXECUTION & STORAGE

ELASTIC RUNTIME

Ops Manager & BOSH

vmware · amazon web services · Windows Azure · Google Cloud Platform · openstack

cf push Green -n demo-time-temp



Pivotal

BLUE/GREEN DEPLOYMENTS

HA Proxy

ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

App Execution (DEA)
Warden
Build packs

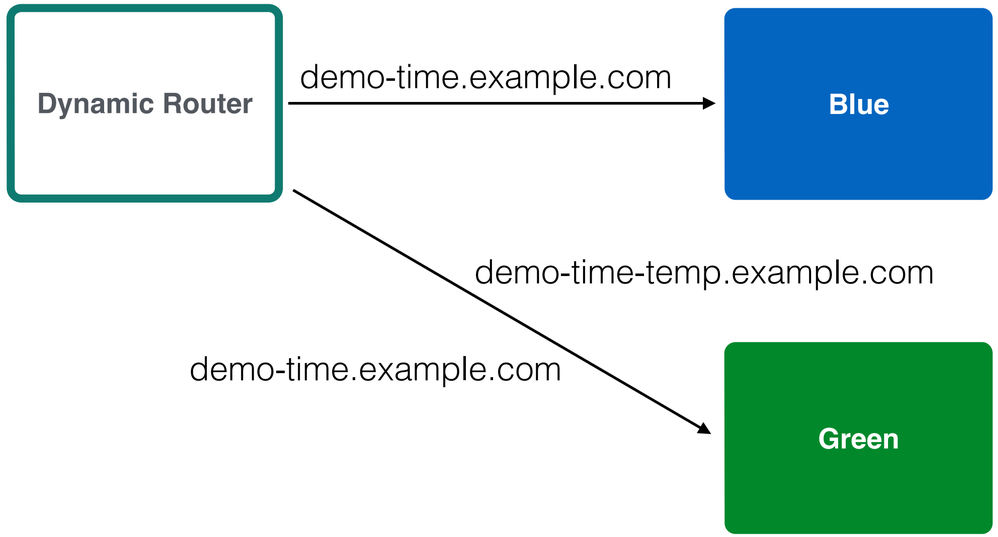
Blob Store — APP EXECUTION & STORAGE

ELASTIC RUNTIME

Ops Manager & BOSH

vmware · amazon web services · Windows Azure · Google Cloud Platform · openstack

cf map-route Green example.com -n demo-time



Pivotal

BLUE/GREEN DEPLOYMENTS

HA Proxy

ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

App Execution (DEA)
Warden
Build packs

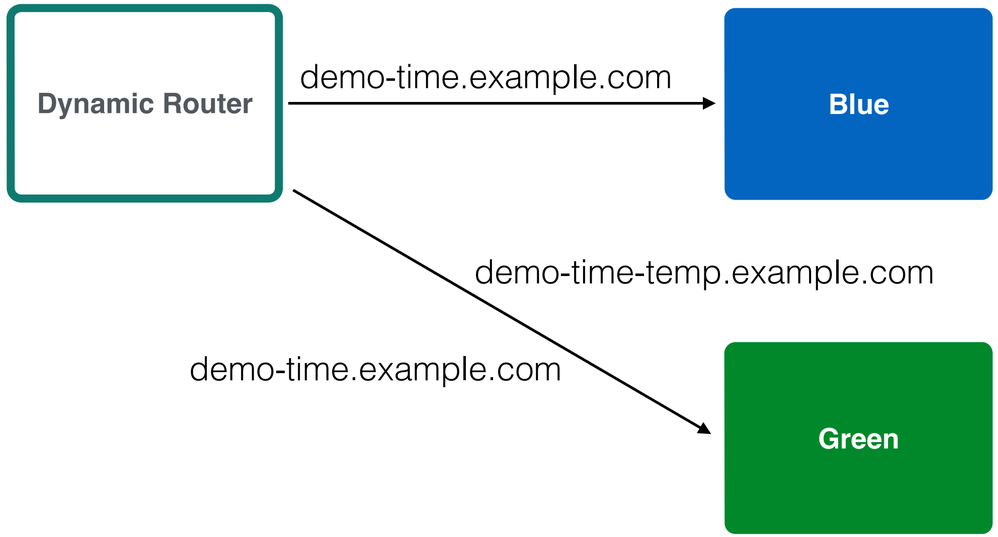
Blob Store — APP EXECUTION & STORAGE

ELASTIC RUNTIME

Ops Manager & BOSH

vmware amazon web services Windows Azure Google Cloud Platform openstack

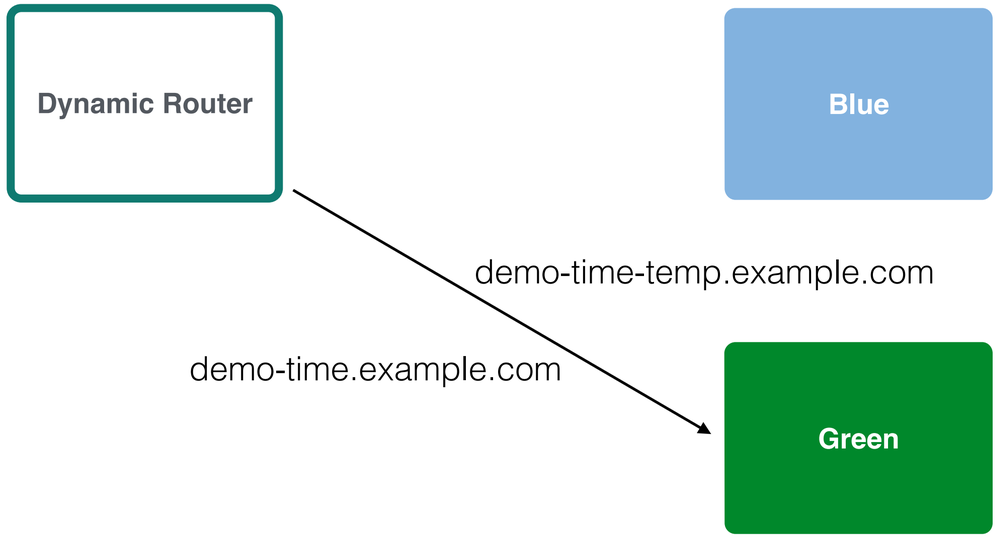
cf unmap-route Blue example.com -n demo-time



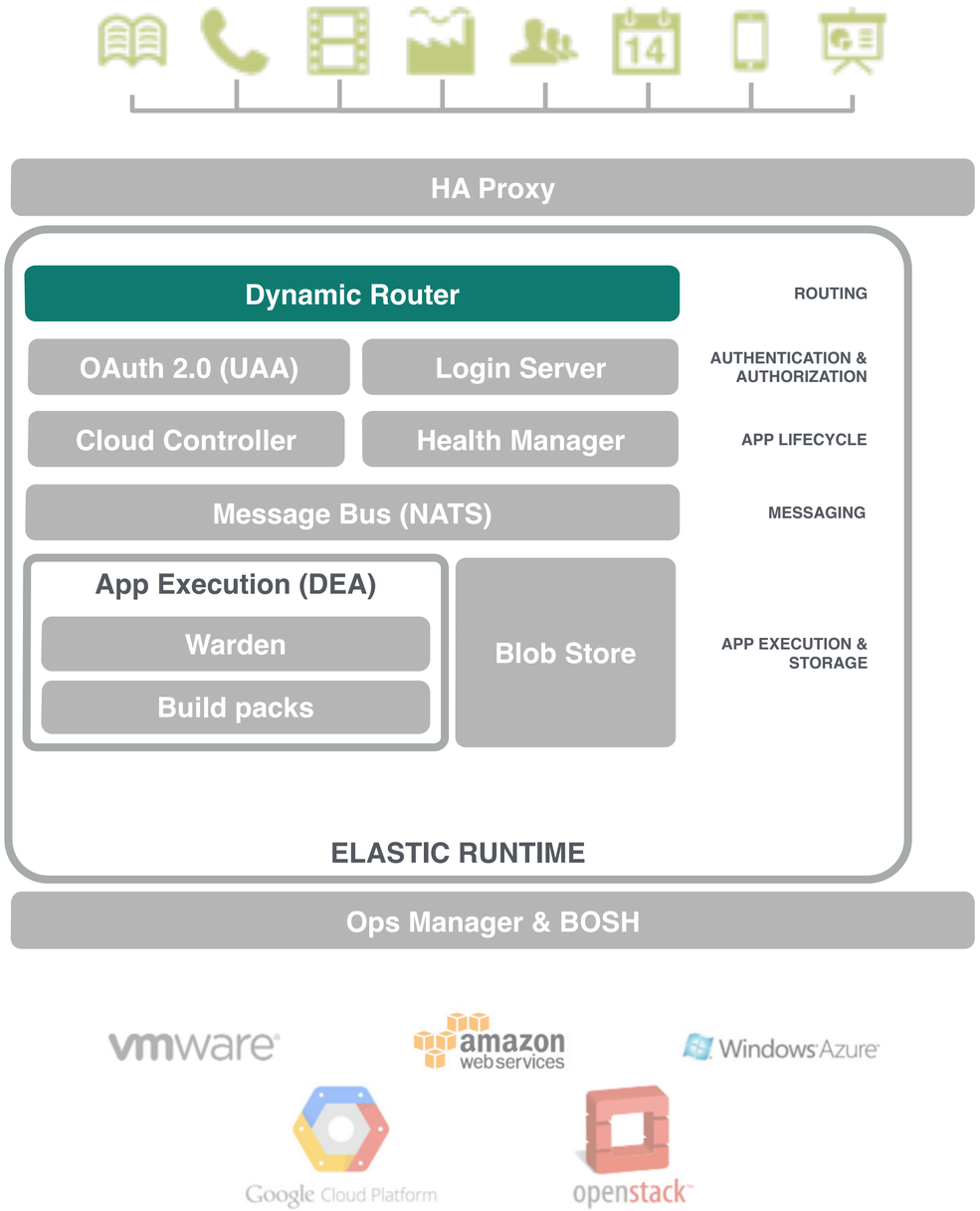
Pivotal

BLUE/GREEN DEPLOYMENTS

cf unmap-route Green example.com -n demo-time-temp



Pivotal



The **router** shapes and routes all external system traffic (HTTP/API) and application traffic from the internet/intranet. It maintains a dynamic routing table for each load-balanced app instance with IP addresses and ports.

HA Proxy

Dynamic Router — ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

App Execution (DEA)
- Warden
- Build packs

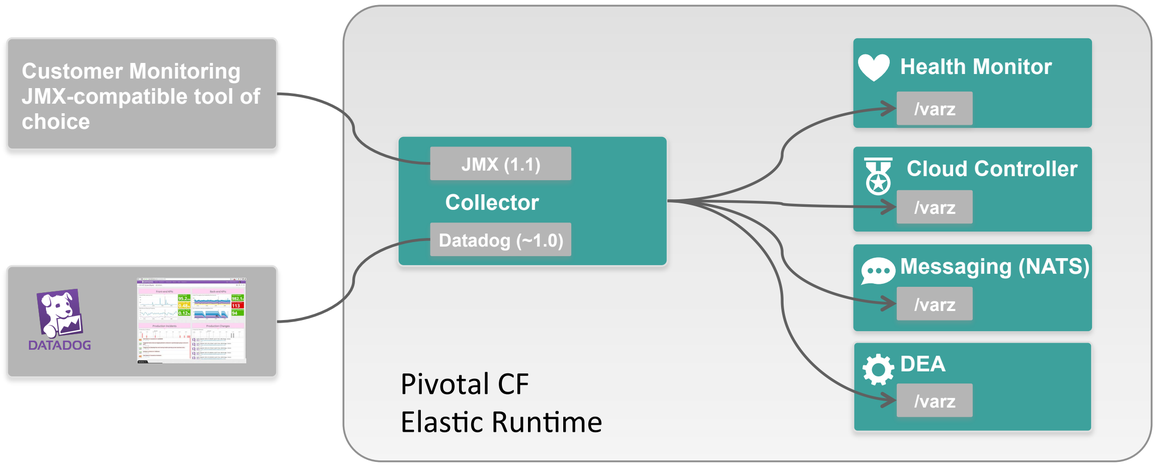
Blob Store — APP EXECUTION & STORAGE

Collector — METRICS & LOGGING

ELASTIC RUNTIME

Ops Manager & BOSH

vmware · amazon web services · Windows Azure · Google Cloud Platform · openstack



Pivotal

HA Proxy

Dynamic Router — ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

App Execution (DEA)
- Warden
- Build packs

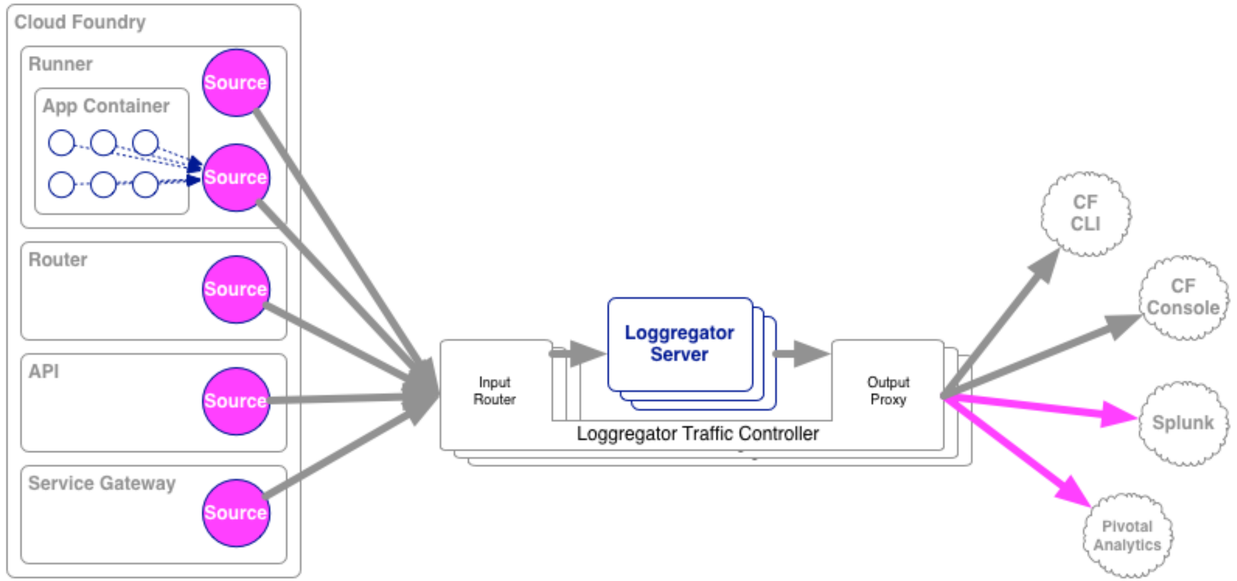
Blob Store — APP EXECUTION & STORAGE

Syslog | Collector | App Log — METRICS & LOGGING

ELASTIC RUNTIME

Ops Manager & BOSH

vmware · amazon web services · Windows Azure · Google Cloud Platform · openstack



https://www.youtube.com/watch?v=rk_K_AAHEEI

Pivotal

HA Proxy

Dynamic Router — ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

App Execution (DEA)
- Warden
- Build packs

Blob Store — APP EXECUTION & STORAGE

Syslog | Collector | App Log — METRICS & LOGGING

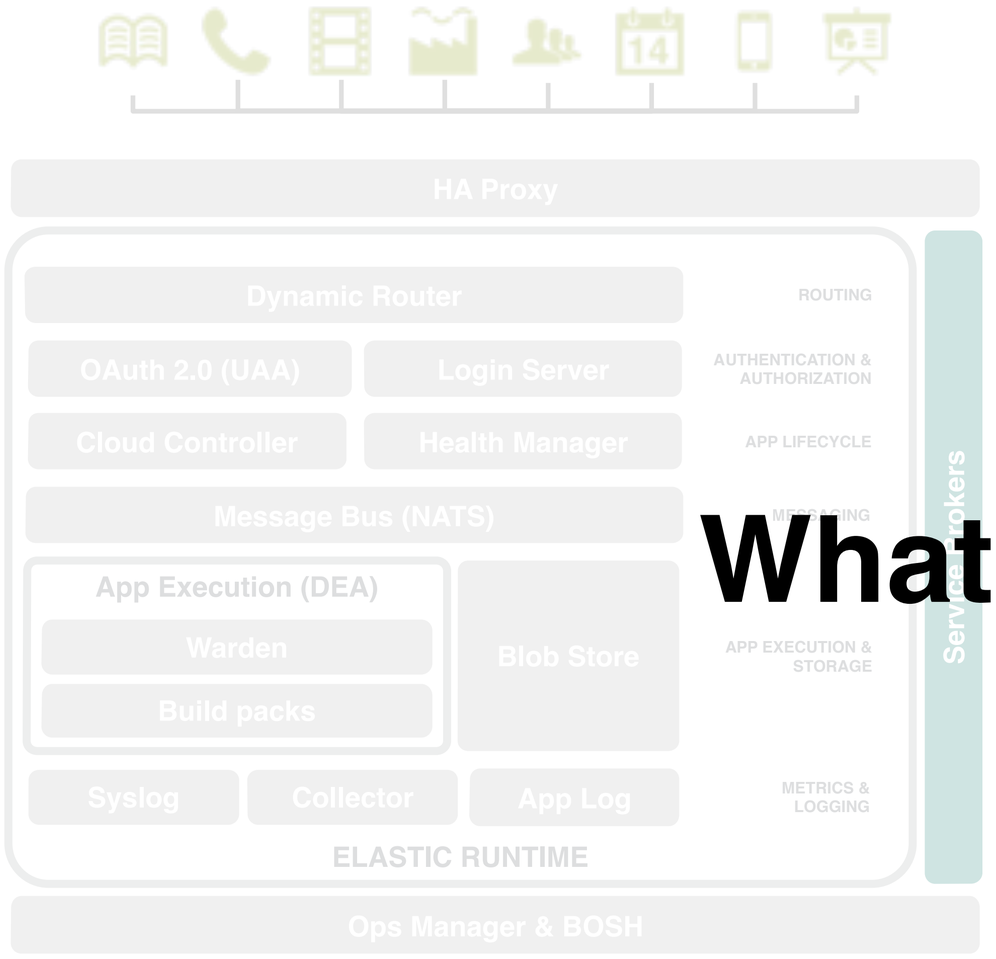
ELASTIC RUNTIME

Service Brokers

Ops Manager & BOSH

vmware · amazon web services · Windows Azure · Google Cloud Platform · openstack

Pivotal



What is a Service?

Service: A conceptual external application dependency made available in the platform (database, message queue, rest endpoint, etc)

Service Plan (catalog): The profile of available offerings for a service, often tiered in nature (i.e. 250MB Redis Service allowing 10 concurrent connections)

Service Instance: An instantiation of a Service and Service Plan made available to applications

Service Binding: A binding between an application and a service instance allowing the application to leverage the instance.

Pivotal

HA Proxy

Dynamic Router — ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

App Execution (DEA)
- Warden
- Build packs

Blob Store — APP EXECUTION & STORAGE

Syslog | Collector | App Log — METRICS & LOGGING

ELASTIC RUNTIME

Service Brokers

Ops Manager & BOSH

vmware · amazon web services · Windows Azure · Google Cloud Platform · openstack

A **Service Broker** implements a published RESTful API and is registered with the Cloud Controller

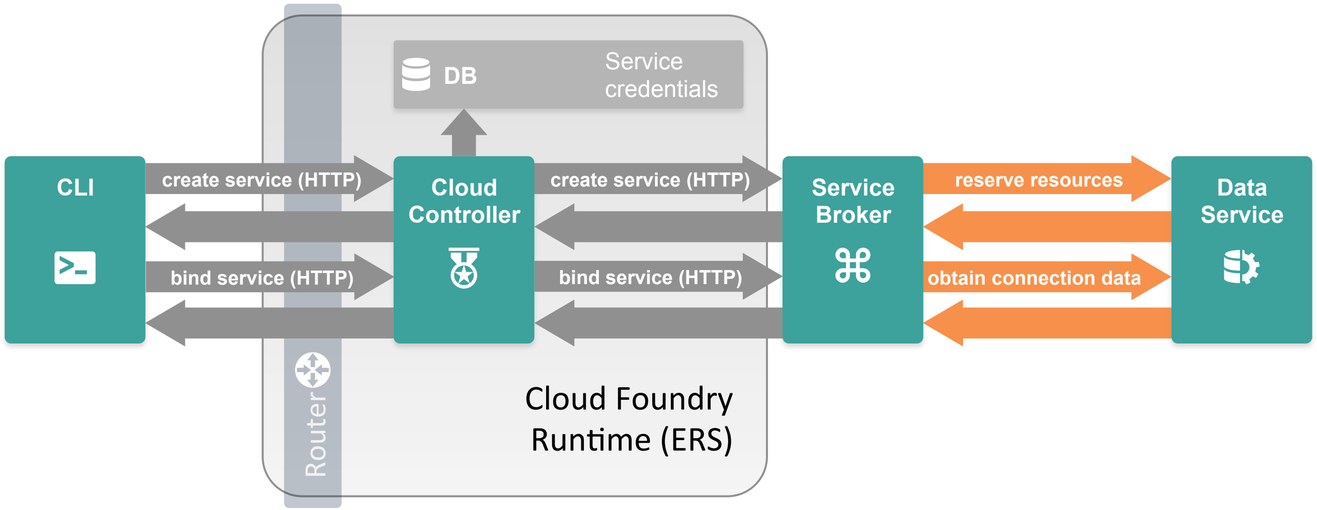
/v2/catalog [GET] – List services and plans available from this broker.

/v2/service_instances/:id [PUT] – Create a new service instance.

/v2/service_instances/:id [DELETE] – Delete a service instance.

/v2/service_instances/:instance_id/service_bindings/:id [PUT] – Create a new binding to a service instance.

/v2/service_instances/:instance_id/service_bindings/:id [DELETE] – Delete a service instance binding (unbind).



Pivotal

HA Proxy

Dynamic Router — ROUTING

OAuth 2.0 (UAA) | Login Server — AUTHENTICATION & AUTHORIZATION

Cloud Controller | Health Manager — APP LIFECYCLE

Message Bus (NATS) — MESSAGING

App Execution (DEA)
- Warden
- Build packs

Blob Store — APP EXECUTION & STORAGE

Syslog | Collector | App Log — METRICS & LOGGING

ELASTIC RUNTIME

Service Brokers

Ops Manager & BOSH

vmware · amazon web services · Windows Azure · Google Cloud Platform · openstack

MANAGED SERVICES

Pivotal HD Service for Pivotal CF
Gain insight from the massive data captured by apps, syst...

API Gateway for Pivotal CF
Create mobile-optimized APIs

Redis for Pivotal CF
Cloud Foundry Redis service for application development a...

Riak CS for Pivotal CF
An S3-compatible object store for Cloud Foundry applications

Push Notifications for Pivotal CF
Add secure push notifications to your mobile apps

Data Sync for Pivotal CF
Secure data store with mobile-optimized access

RabbitMQ Service for Pivotal CF
Give your applications a common platform to safely send

MongoDB for Pivotal CF
MongoDB Data Store

MySQL for Pivotal CF
MySQL database-as-a-service for Cloud Foundry applications

App Autoscaling for Pivotal CF
Scales bound applications in response to load

Cassandra for Pivotal CF
Cassandra KV and Table Store

Elasticsearch for Pivotal CF
Elasticsearch Search Engine

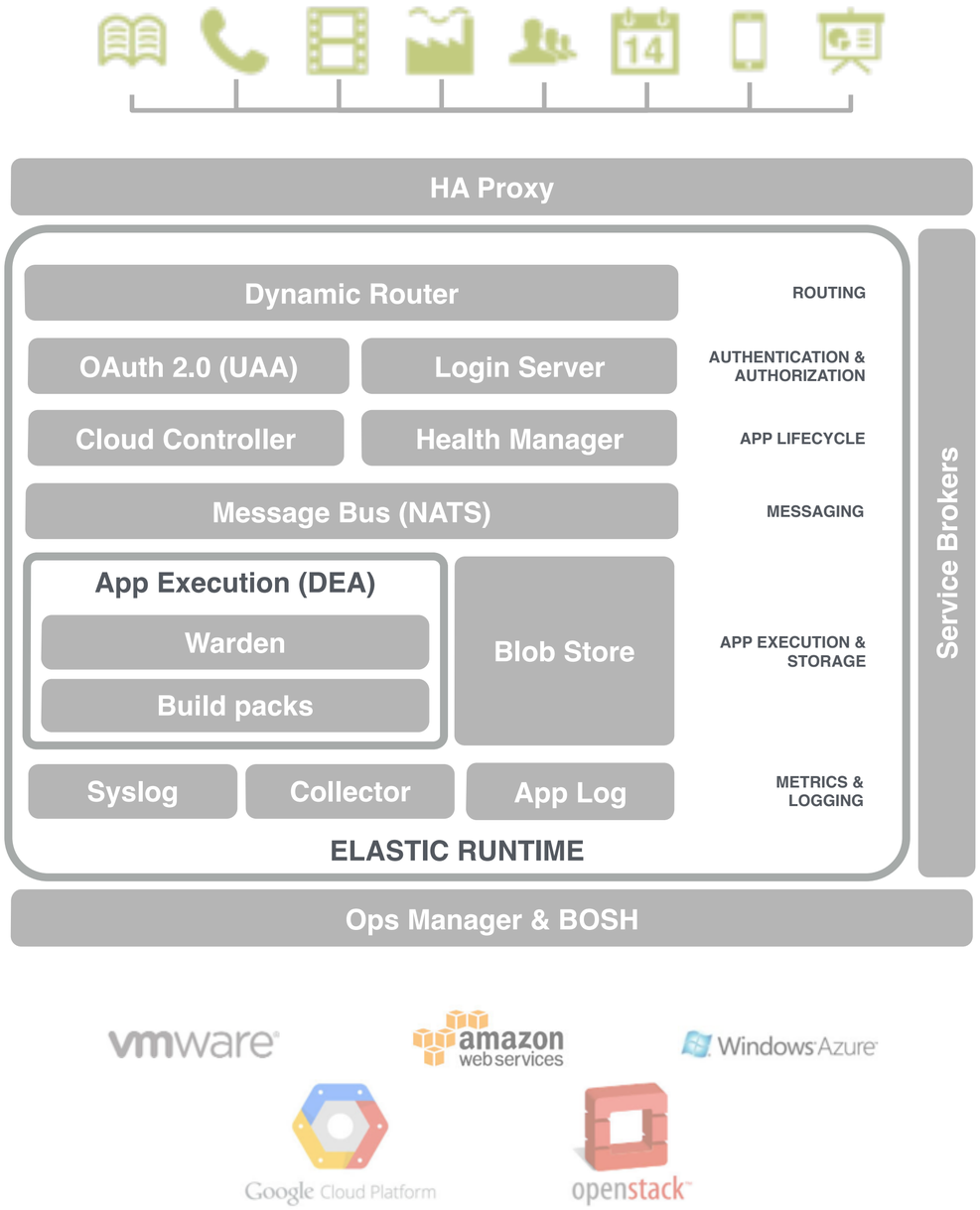
Jenkins Enterprise by CloudBees
Continuous Integration and Delivery for Software

Memcached for Pivotal CF
Memcached Elastic Cache Service

Neo4j for Pivotal CF
Neo4j Graph Database

Pivotal Spring Insight
Zero touch instrumentation of Java applications

Pivotal



User-provided service instances are service instances which have been provisioned outside of Cloud Foundry

- Behave like other service instances once created
- Familiar commands (‘create-service’) provide service instance configuration (including credentials) to applications, eliminating the need to hard code service instance endpoints

Pivotal

RECAP: WHO CAN DESCRIBE THE CORE TENETS OF CLOUD FOUNDRY?

Pivotal CF: Cloud Independent Enterprise PaaS

Simple, Developer Friendly Commands & API

- Auto-detect frameworks
- "Push and it works"
  - .WAR
  - Dockerfile
  - .NET
- Simple service binding
- Agile micro-services

Extensible Framework "Buildpack" Architecture

Operational Benefits for Every Application

- Instant Dynamic Routing
- Log Streams & Aggregation
- Access Controls & Policies
- APM and Auto-scaling
- 4 Layers of High Availability
  - *App-Instance*
  - *Availability Zone*
  - *Process*
  - *Virtual Machine*

Built-in and Ecosystem Services

- Elastic Hadoop
- Mobile
  - Push, Sync, API
- MySQL HA
- Redis
- Rabbit MQ
- ElasticSearch
- MongoDB
- Cassandra
- Jenkins (CI)
- PHD
- And More…

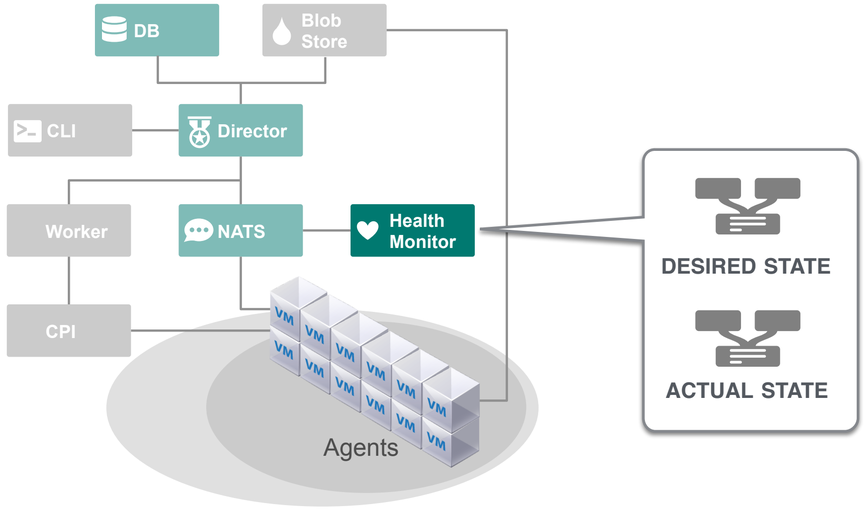
Extensible Service Broker Architecture

Deploy, Operate Update, Scale Platform on Any IaaS

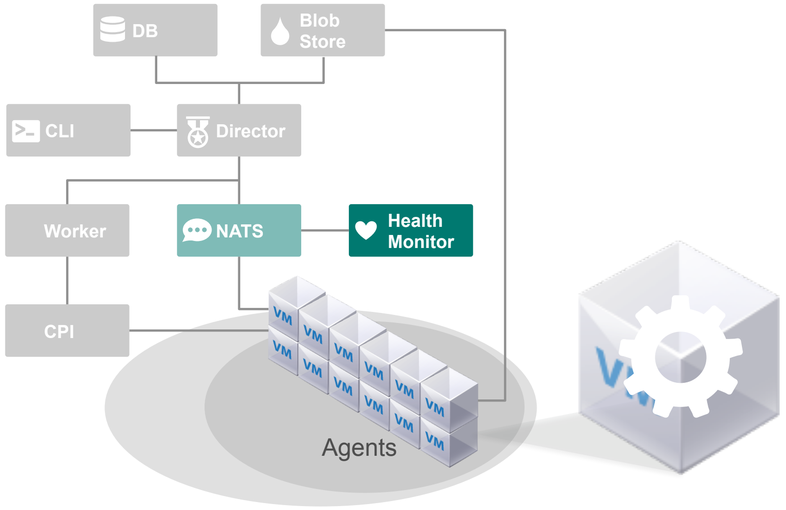
vmware · amazon web services™ · openstack · Google Cloud Platform · ….and more

RECAP: WHO CAN DESCRIBE THE 4 LEVELS OF AVAILABILITY IN CLOUD FOUNDRY?

4 Levels of High Availability

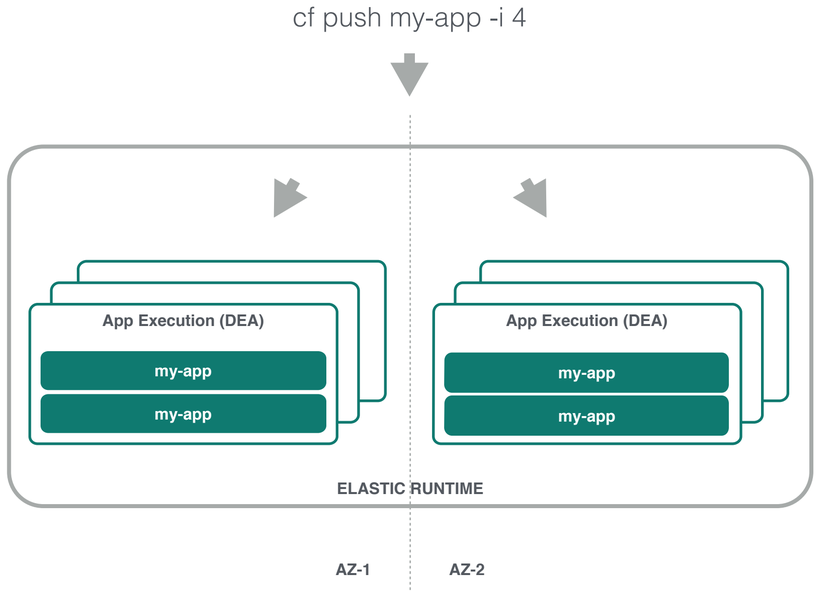


Failed VMs are Recovered

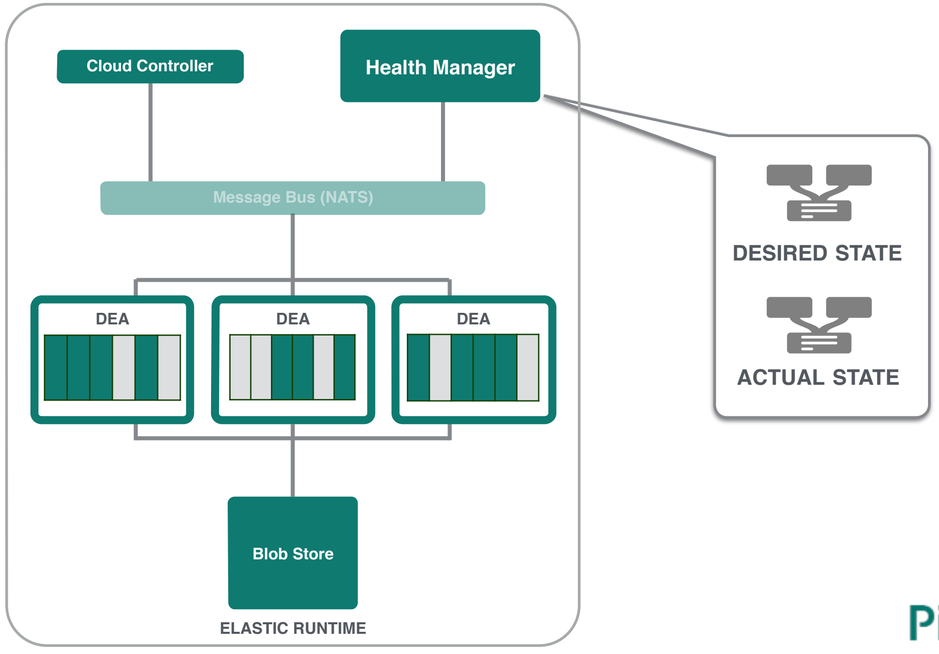


Failed Processes are Recovered

Application Instances Balanced across Availability Zones



Failed Application Instances are Recovered



Pivotal

A NEW PLATFORM FOR A NEW ERA