PCF Security

Pivotal

Platform Trust

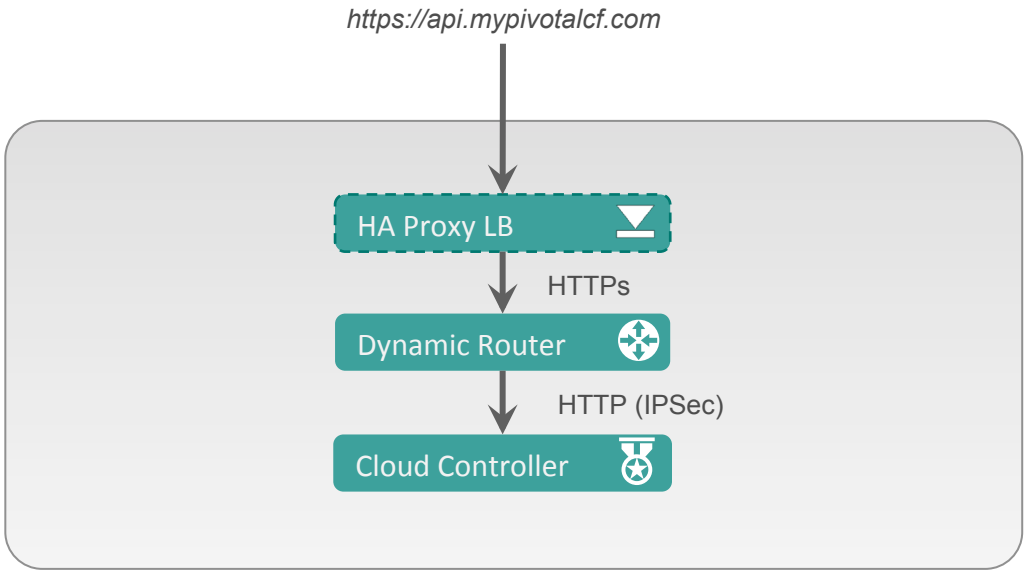
- Explicit, known dependencies
- Homogeneity in the environment, no drift
- Combined CVE / vulnerability management
- 0-downtime deployments and upgrades
- Federated login with enterprise directories
- Control access to services and other resources policy-based egress control
- Enforce policies (server, runtime, libraries, etc.)
- IPSec on every network segment
- RunC integration for AppArmor and user namespaces
- Addition of agent-based monitoring support
- File Integrity Monitor
- Application dependency monitor

System Boundaries and Access

Pivotal

API Access

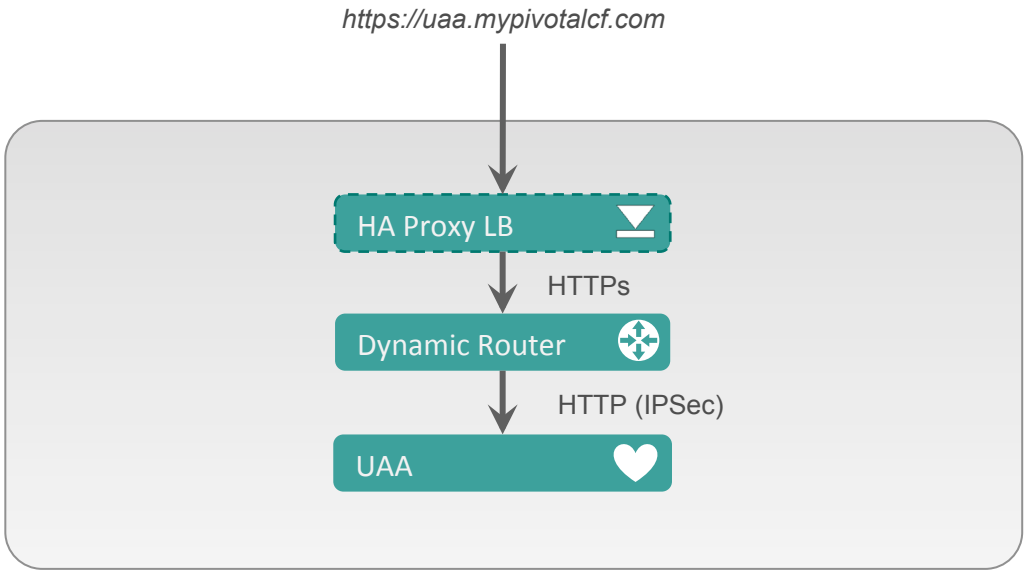
API access (app management, service management, org/space management, etc.) is routed to Cloud Controller via HTTPS



Pivotal

Token Acquisition

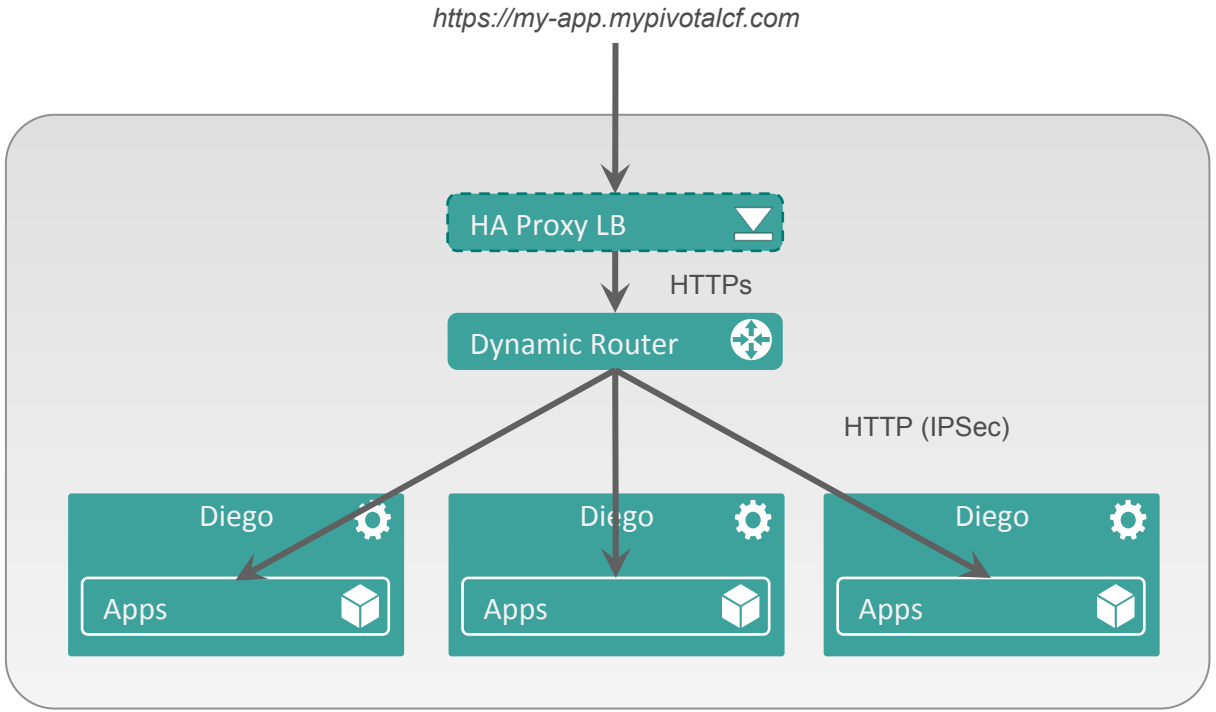
Federates with enterprise login systems. Standard protocols.



Pivotal

Application Access

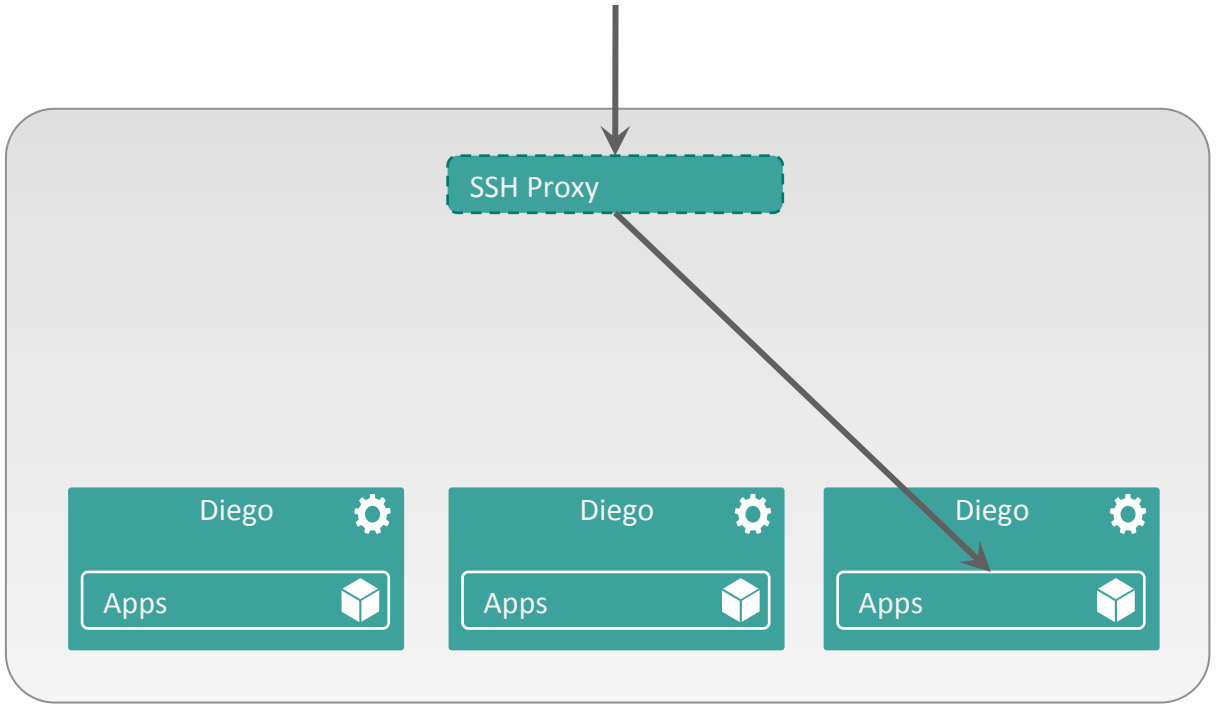
Application access is routed directly to an application instance via round robin algorithm.



Container Access

Optionally allow SSH access to running containers.

Merges user identity with SSH access (vs. separate management of SSH keys).

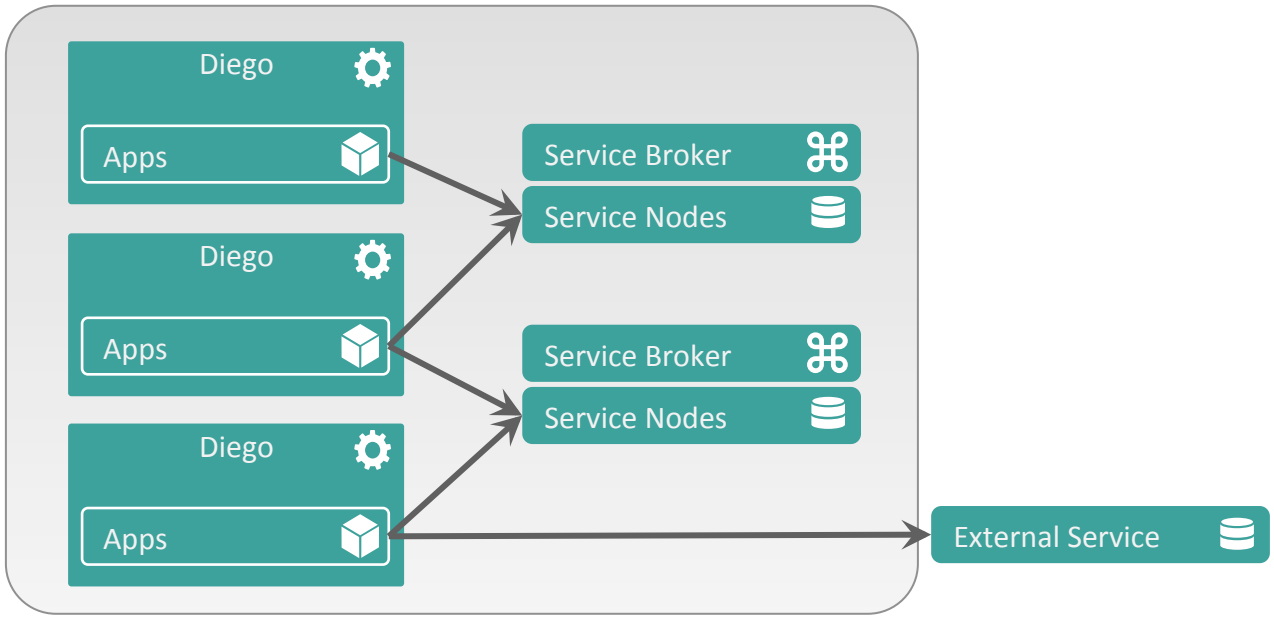


Pivotal

Service Access

Applications connect directly to managed services via assigned addresses and ports

Applications can access services outside of the PCF VLAN



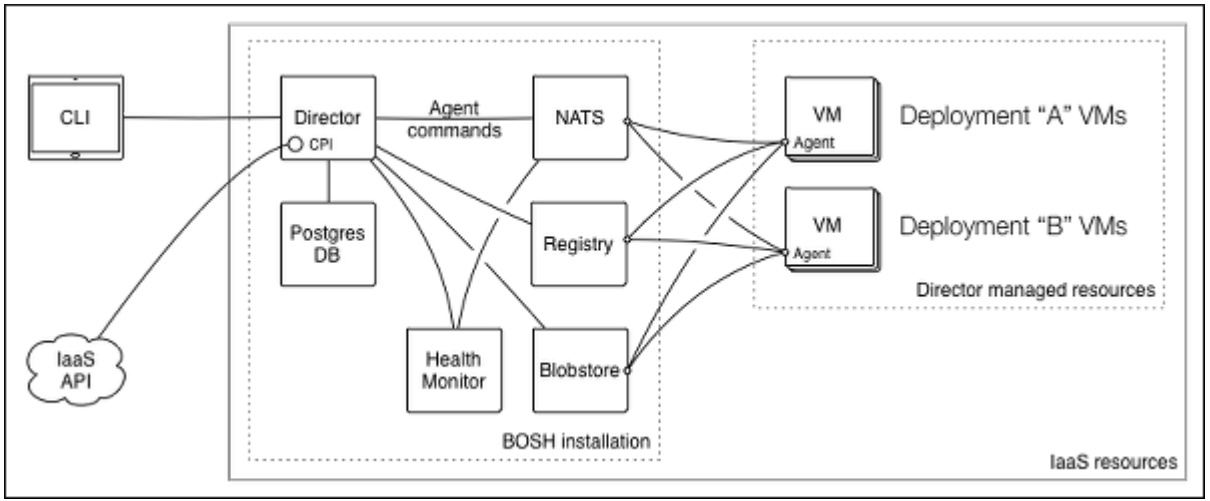
Pivotal

BOSH Access

Director, agents, and CLI

Single, locked down Stem Cell VM image

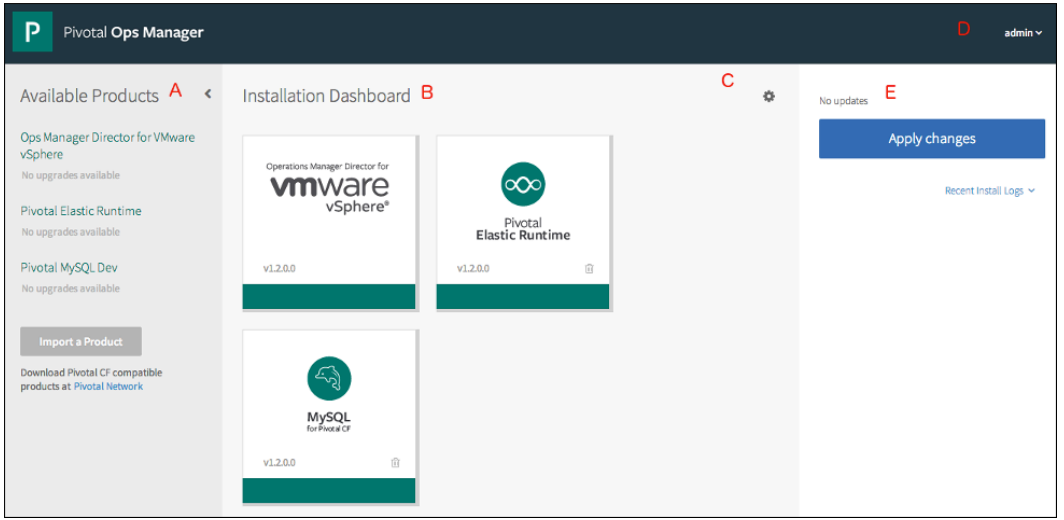
Cookie cutter, reliable VM creation, software deployment, and management



OpsManager Access

Automates BOSH, simplifies deployments, expose services, etc.

Federates with UAA for login.



Pivotal

Application Containers

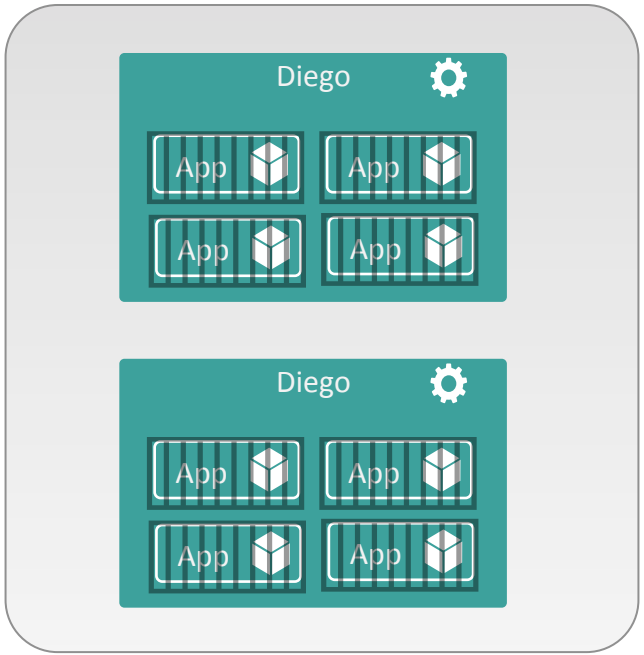
Pivotal

Container Isolation

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

RunC, AppArmor, and user namespaces

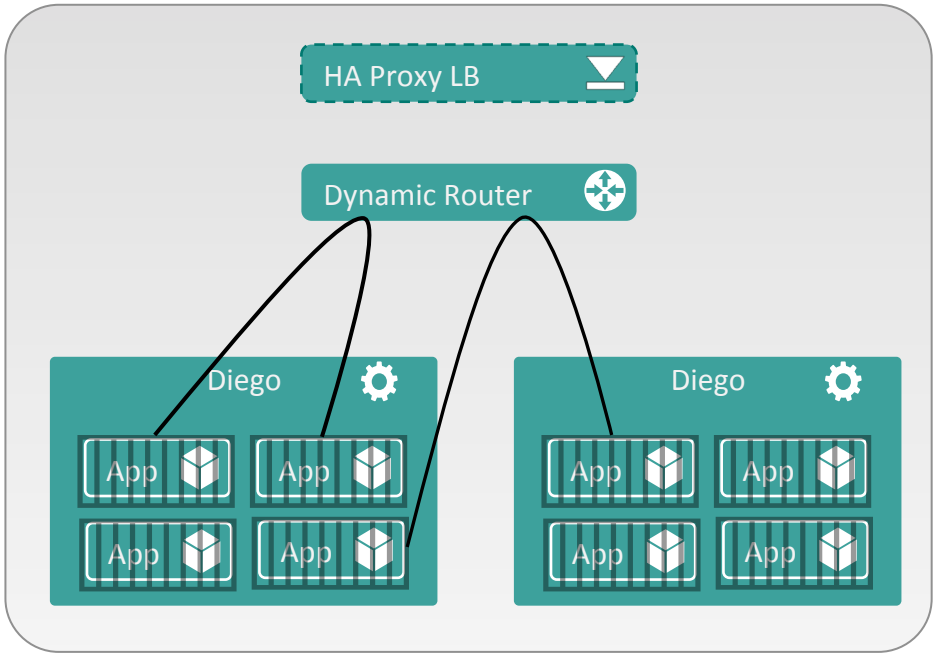
Containers have their own private network, not accessible from outside the Diego Cell



Container Isolation

Routers forward requests from outside using the app's route to the assigned port on the cell, 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

Application Security Groups

Pivotal

Security Groups

- Groupings of network egress access rules for application containers
- All via the Cloud Controller API
  - operators/admins can create and apply security groups
  - space users can view rules

Pivotal

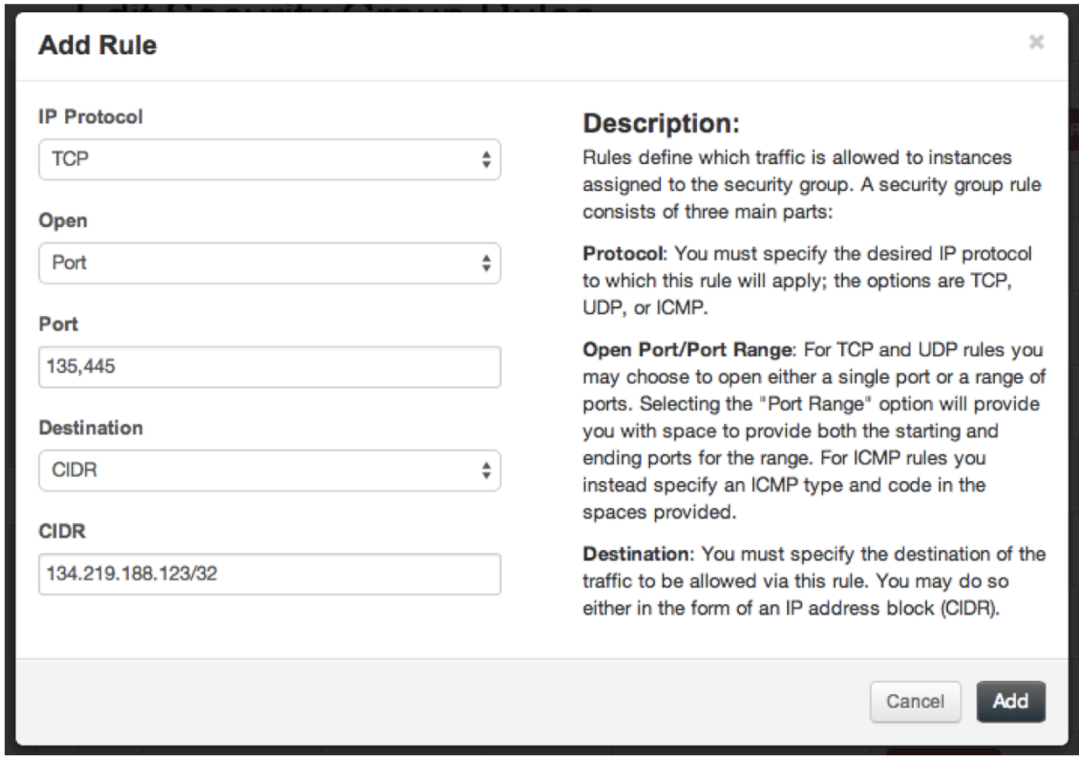
Assigning Security Groups

- System security rules (REJECT all) are hard-coded at the bottom of the chain
- Default global security groups can be applied at the platform level
  - application staging
  - application runtime
- Additional security groups can be applied to individual space and are inserted as whitelisted endpoints earlier in the chain

Pivotal

Security Group Rules

- Security group rules are whitelist rules



Pivotal

Service Credentials

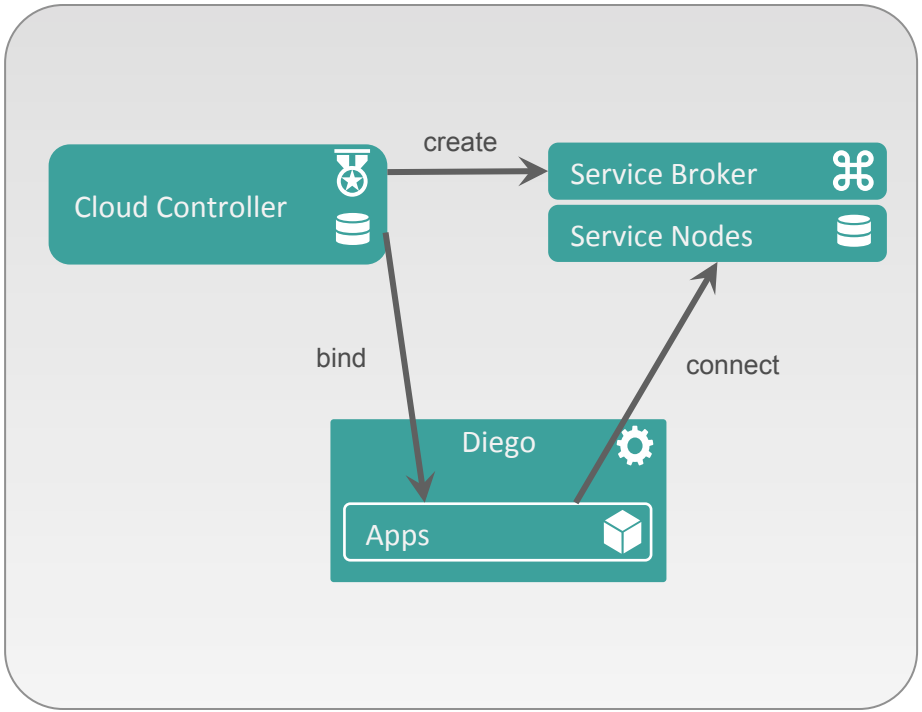
Pivotal

Managed Services

Service Brokers generate connection details and credentials for managed services

CC encrypts and stores credentials in CCDB

Credentials injected into containers 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"
   }
  }
 ]
} "
```

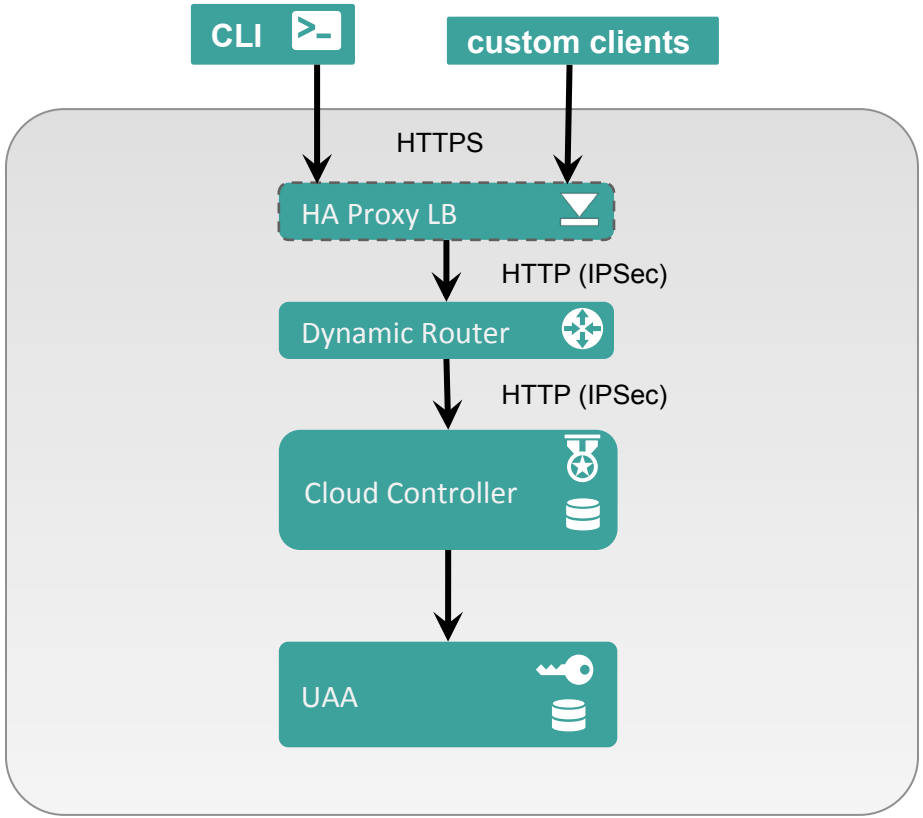
Pivotal

Identity and Access Control

Pivotal

End-User Identity

- UAA handles authentication
  - by default, stores usernames and passwords in CCDB
  - supports LDAP and Federated integration
- UAA is an OAuth2 auth server
  - manages access and refresh tokens
- All API interactions include a valid OAuth2 access token



Pivotal

VM Access

Operations Manager creates randomized passwords for access to all managed VMs

VM credentials are visible in the Operations Manager UI

(this is changing)

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

BUILT FOR THE SPEED OF BUSINESS