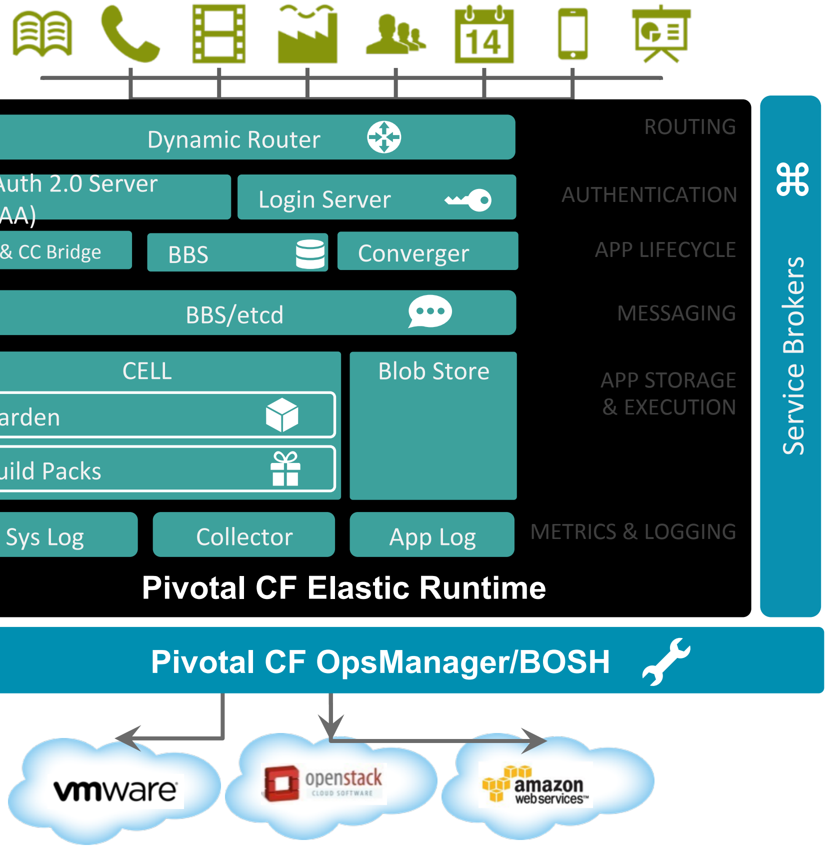
Security

Access Control, Application Security Groups and Identity Management

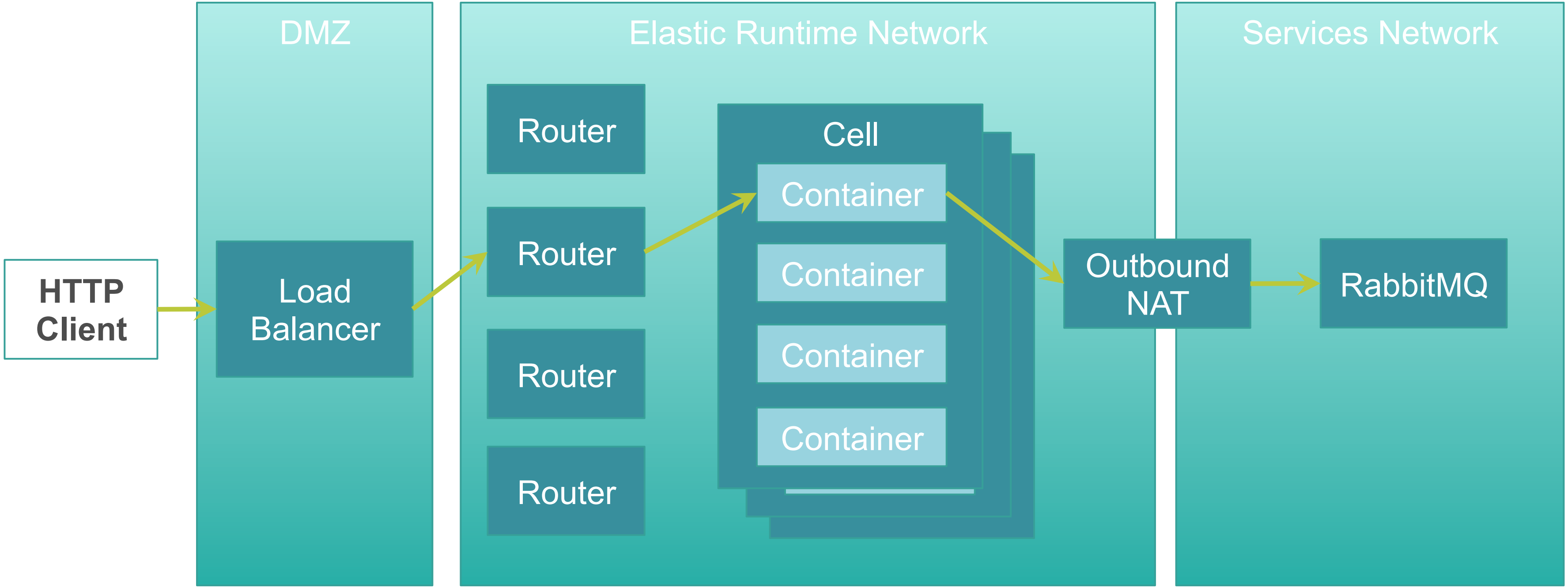
Data Protection

Data-in-Motion, Data-at-Rest

Elastic Runtime High Level Architecture



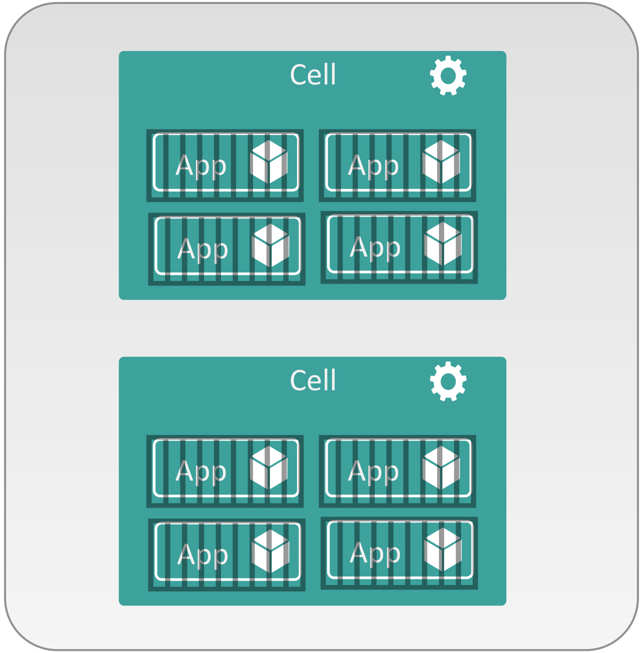
ER Ingress Networking Traffic Example



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 Cell



Data-at-Rest

- In the ER – two main points of non-ephemeral storage:
  - CCDB – Centralized storage for application metadata, includes access information for services leveraged by the application containers.
  - BLOB Store – Stores container images, application artifacts
- Both can be externally managed and configured.

Network Surface Area

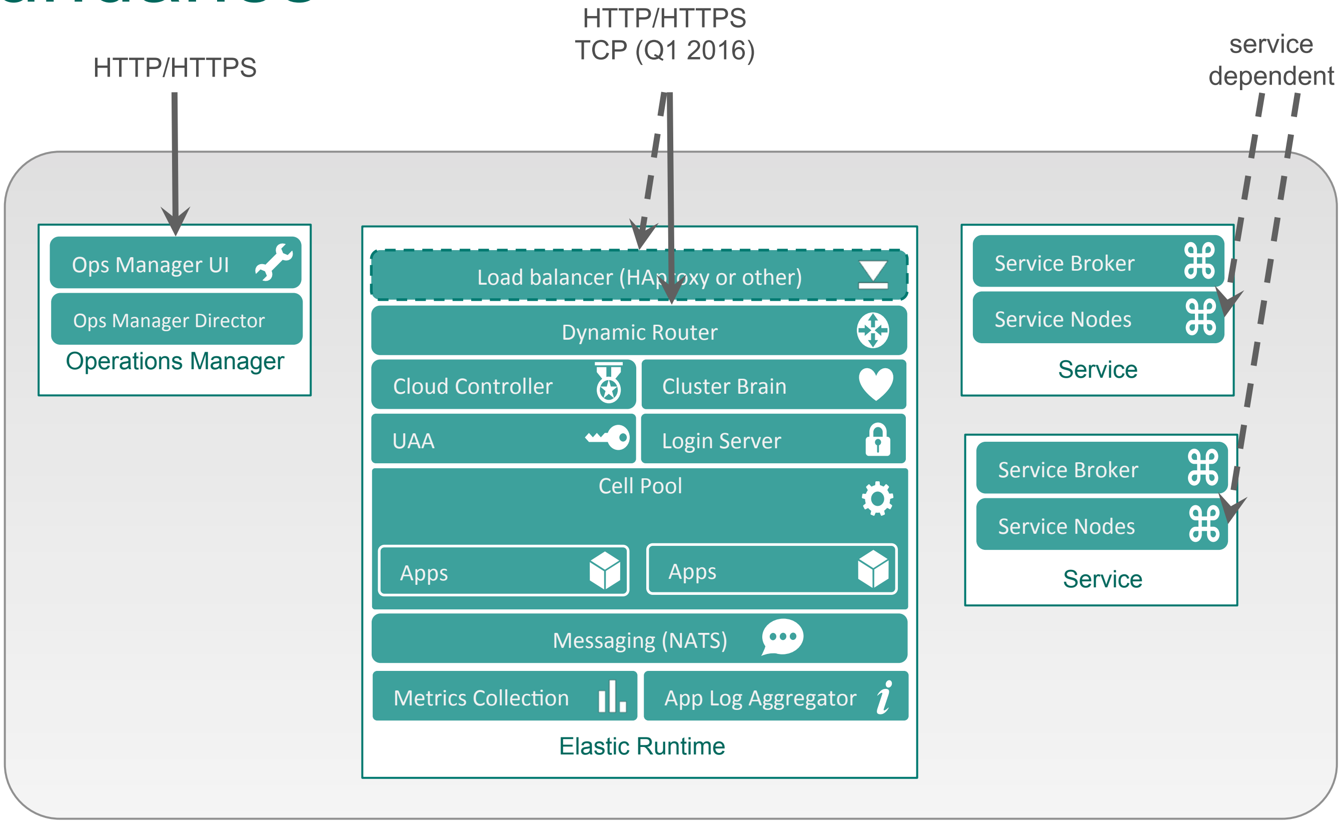
Getting Access via Network Endpoints, Controlling Access via AuthZ and AuthN

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

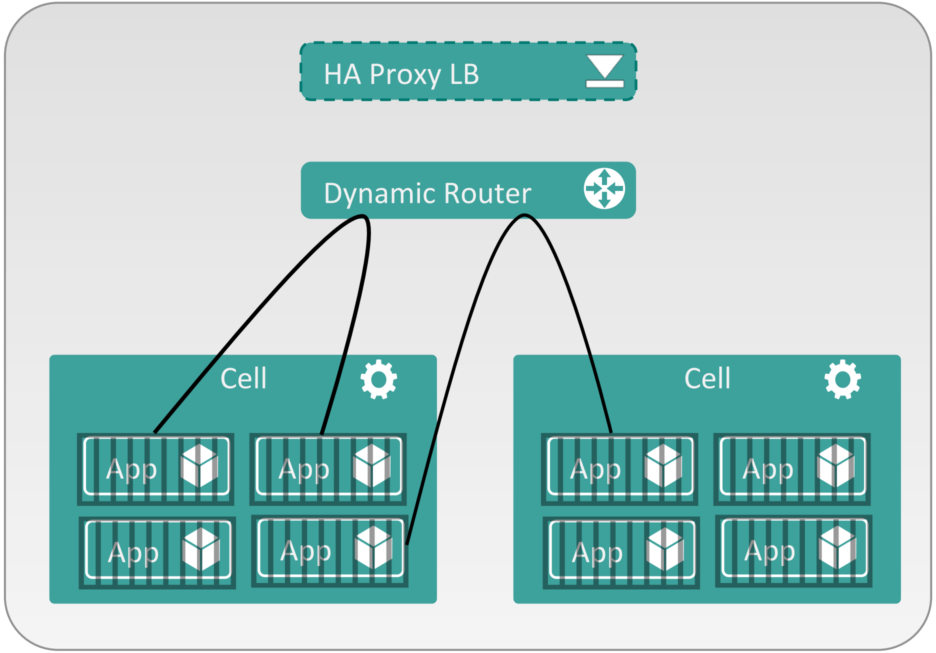


Pivotal

Container Isolation

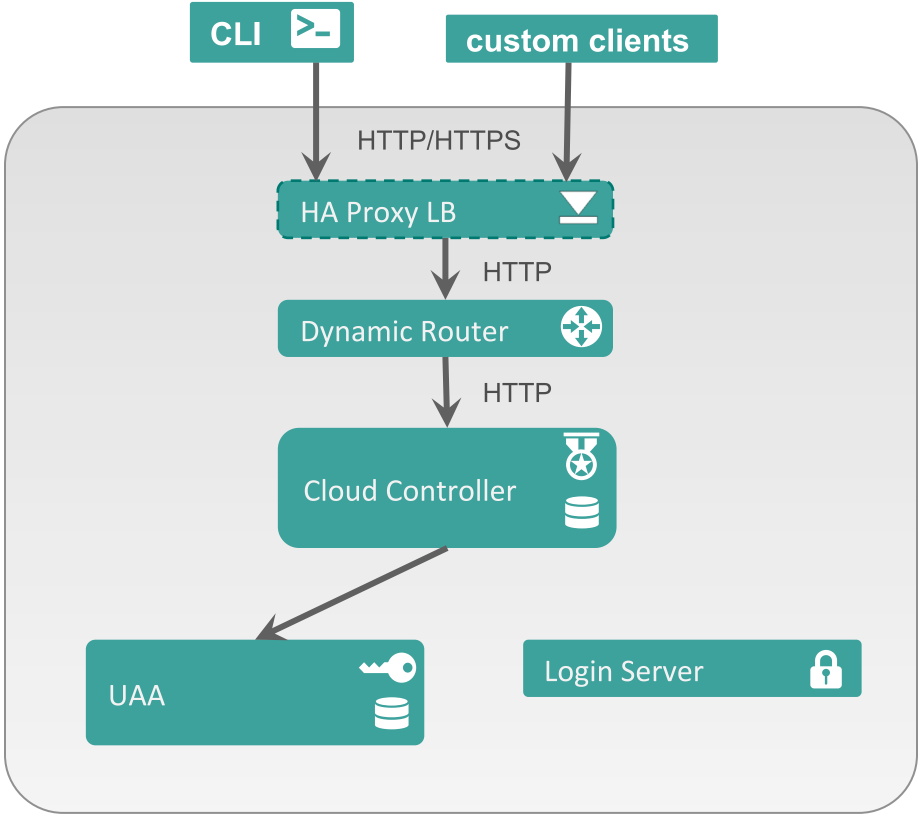
Routers forward requests from outside using the app's route to the assigned port on the Cell, which does network translation to the container's internal IP and port

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



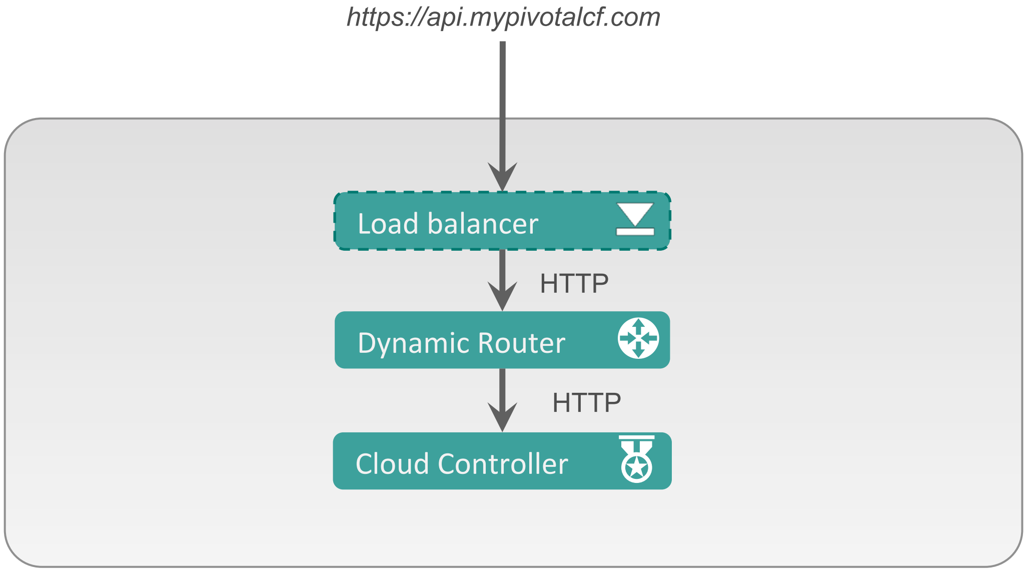
End-User Identity

- Multitenant UAA/Login Server handles authentication
  - LDAP/AD integration
  - Identity Zones provides unique, isolated sub-domains
- UAA is an OAuth2 token server
- All interactions with the API must include a valid OAuth2 access token



API Access

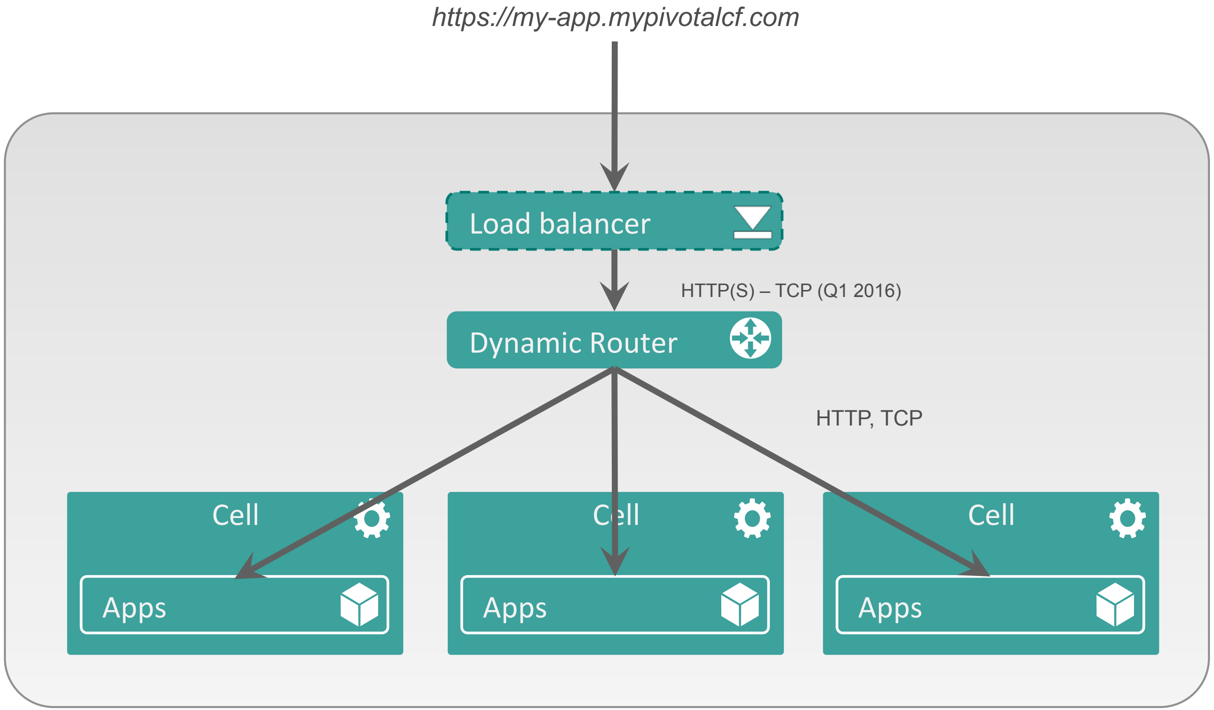
API access (app management, service management, org/space management, etc.) is routed to Cloud Controller via HTTP/ HTTPS



Application Access

Application access is routed directly to an application instance for any number of domans

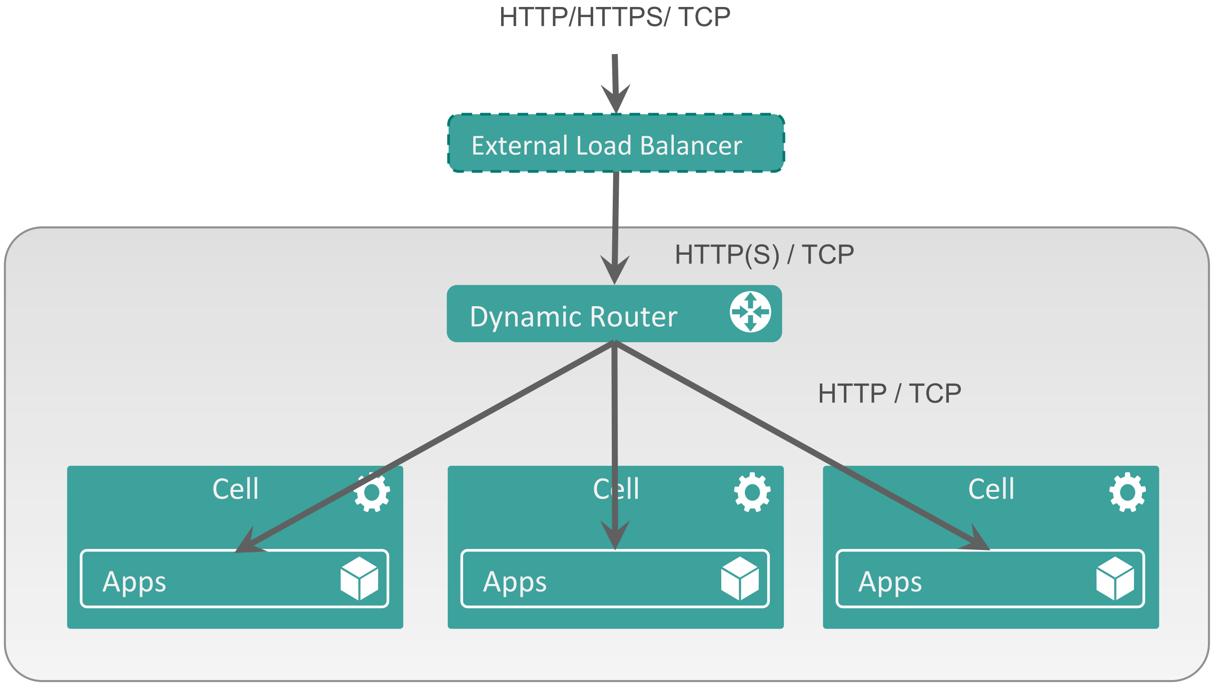
SSL is terminated at the load balancing layer; optionally at the routing layer; all internal PCF traffic is trusted HTTP (or TCP in PCF 1.7+)



External Load Balancer

HA Proxy can be replaced with an external Load Balancer

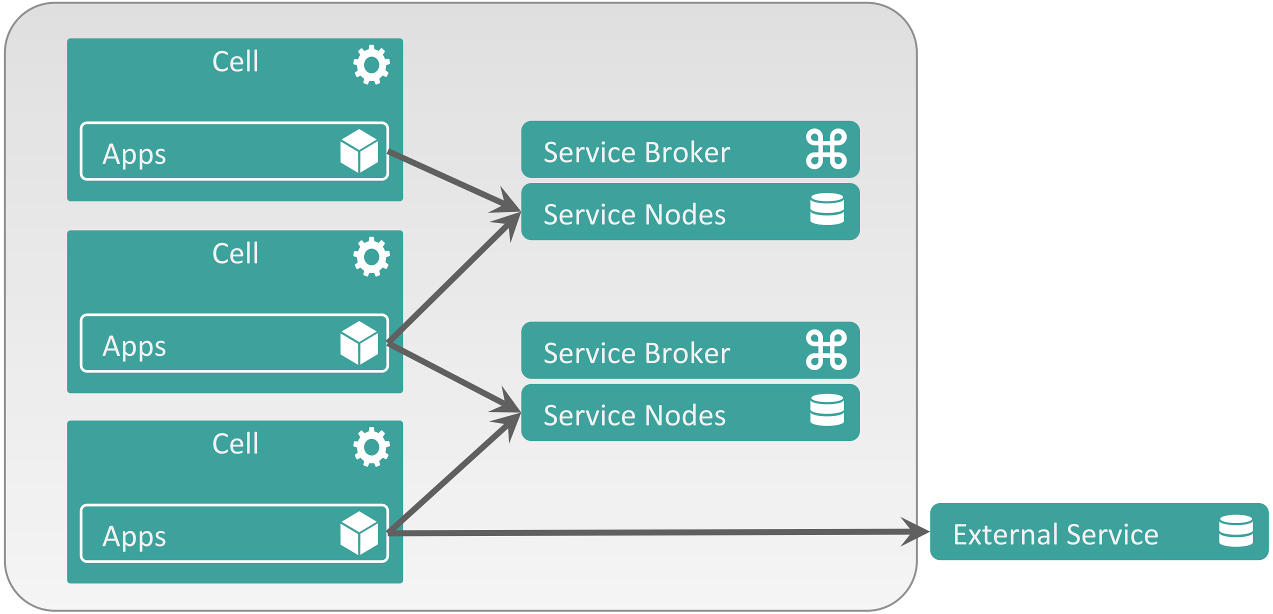
SSL is terminated at the Load Balancer and/or Router



Service Access

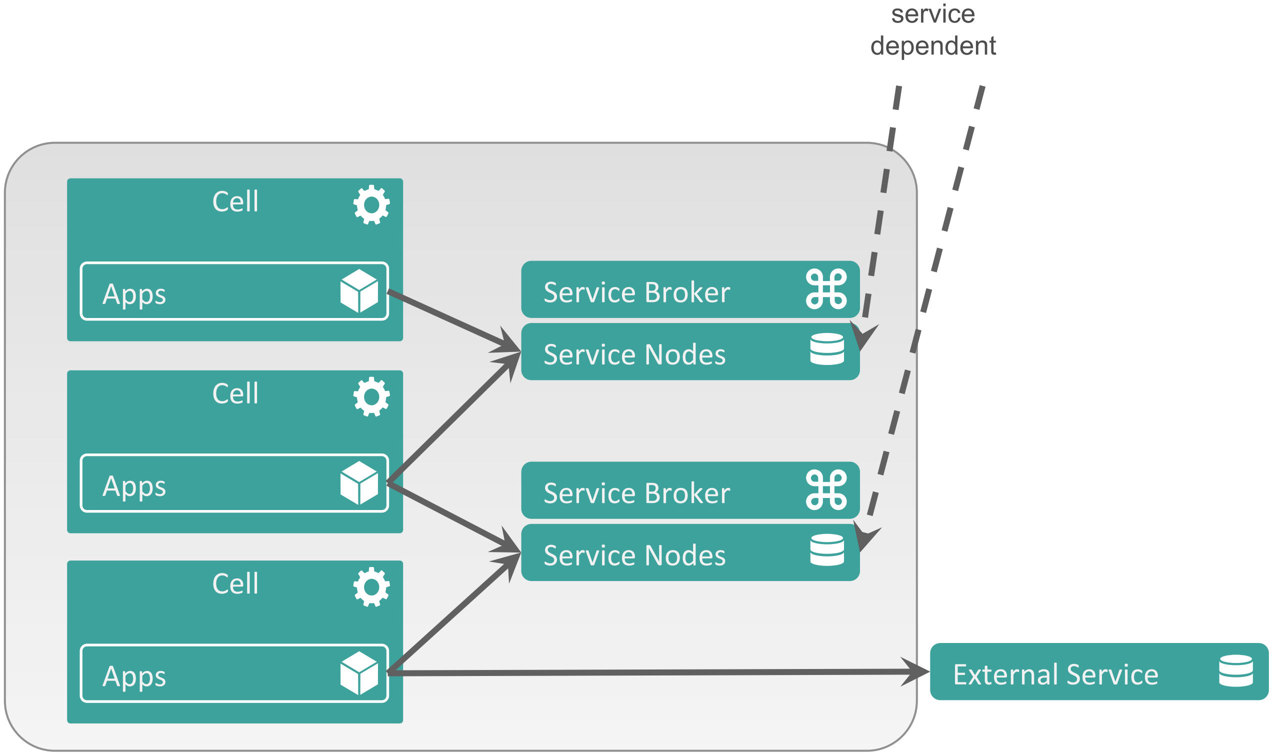
Applications connect directly to managed services via assigned addresses and ports

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

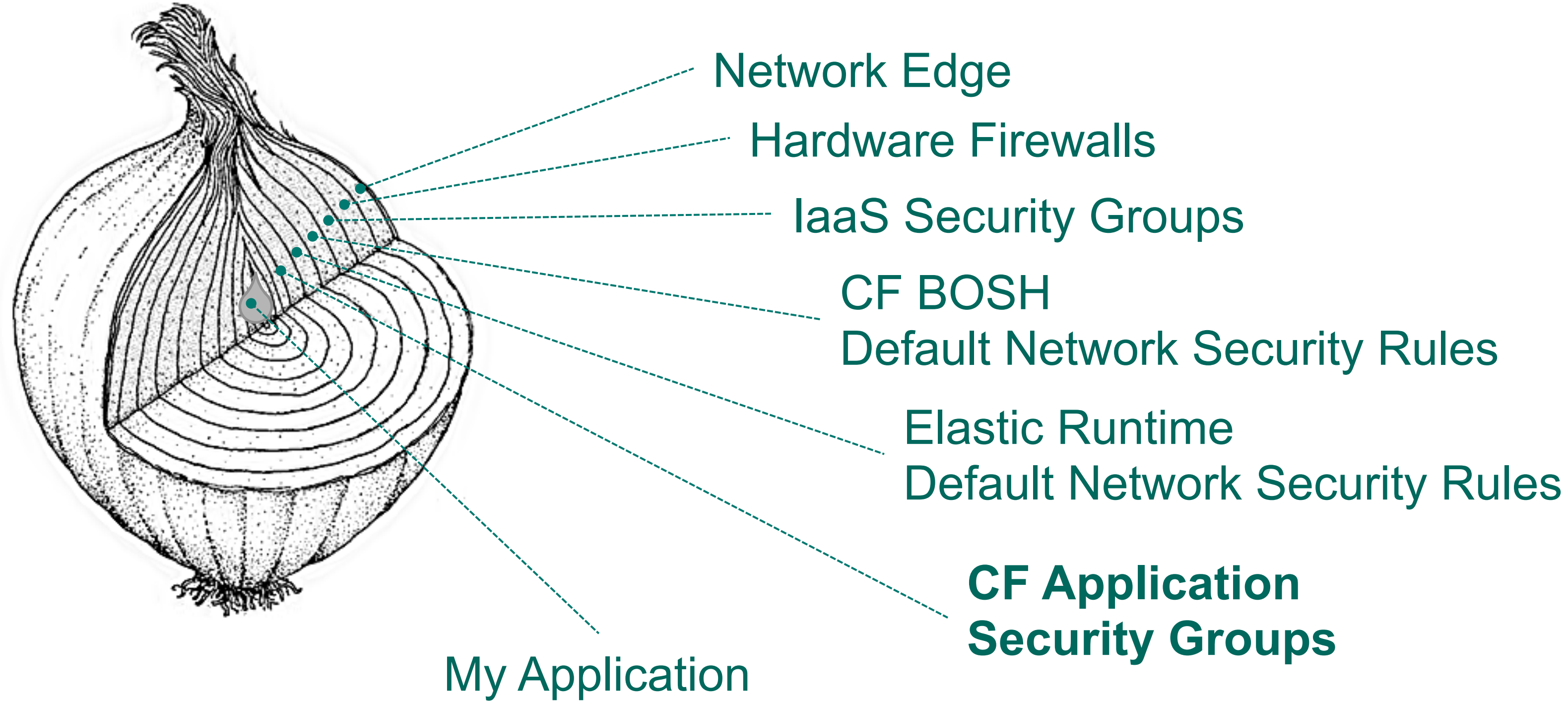


Service Access

- 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



Security Groups – A Layered Approach



Network Edge

Hardware Firewalls

IaaS Security Groups

CF BOSH
Default Network Security Rules

Elastic Runtime
Default Network Security Rules

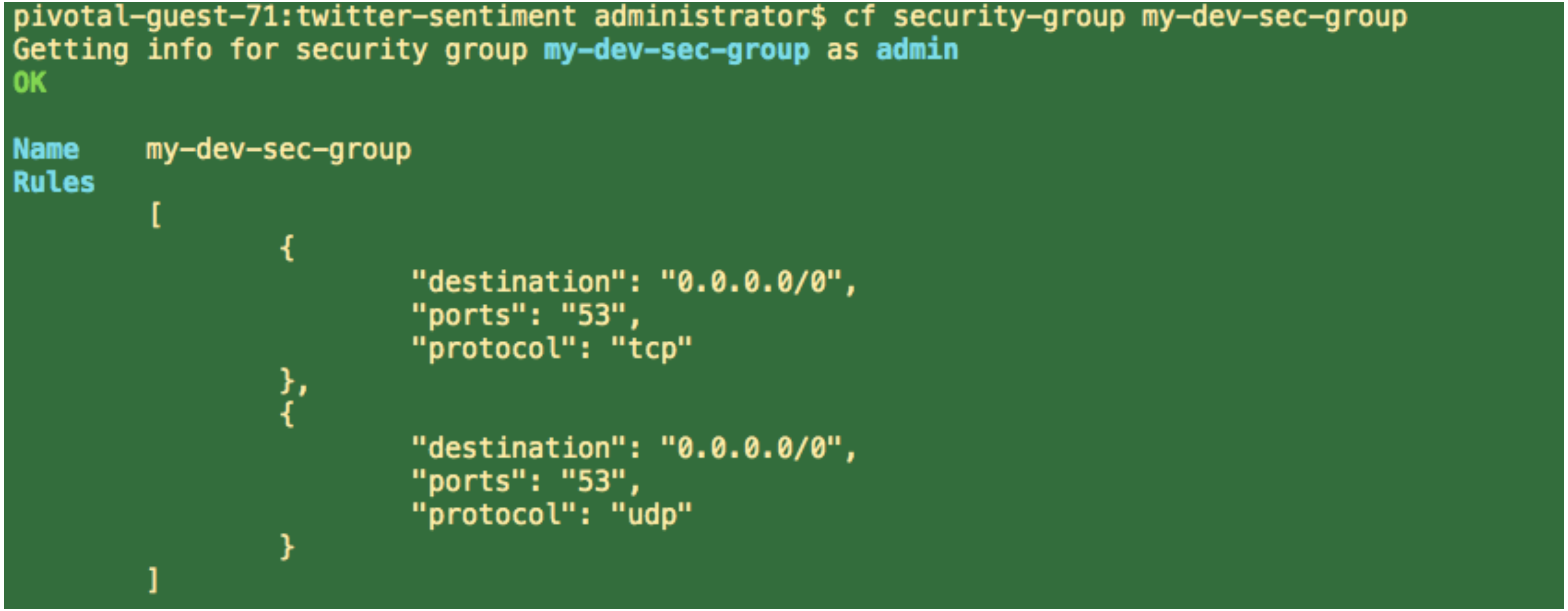
CF Application
Security Groups

My Application

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

Security Group - Example

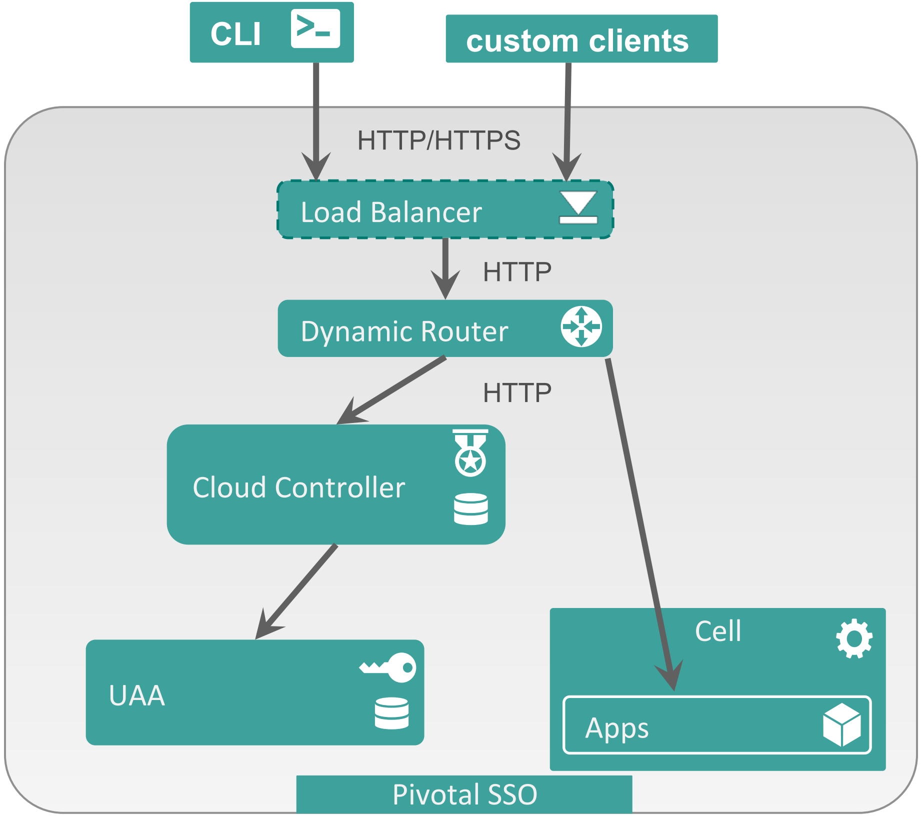


```
pivotal-guest-71:twitter-sentiment administrator$ cf security-group my-dev-sec-group
Getting info for security group my-dev-sec-group as admin
OK

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"
                }
        ]
```

End-User Identity

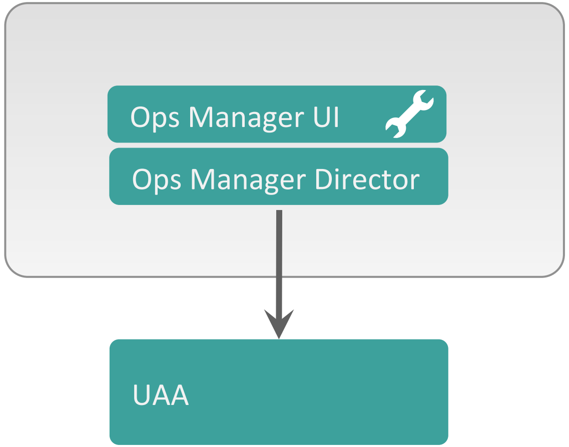
- UAA is an OAuth2 token server
  - Handles web authentication
  - manages access and refresh tokens
  - by default, stores usernames and passwords in CCDB
  - LDAP/AD integration
  - SAML SSO Integration
- All interactions with the API must include a valid OAuth2 access token
- All applications can integrate with Pivotal Single Sign On services for their own Oauth2 identity zones



Operator Identity

Operations Manager <= 1.6 supports a single username and password for access to operations functions

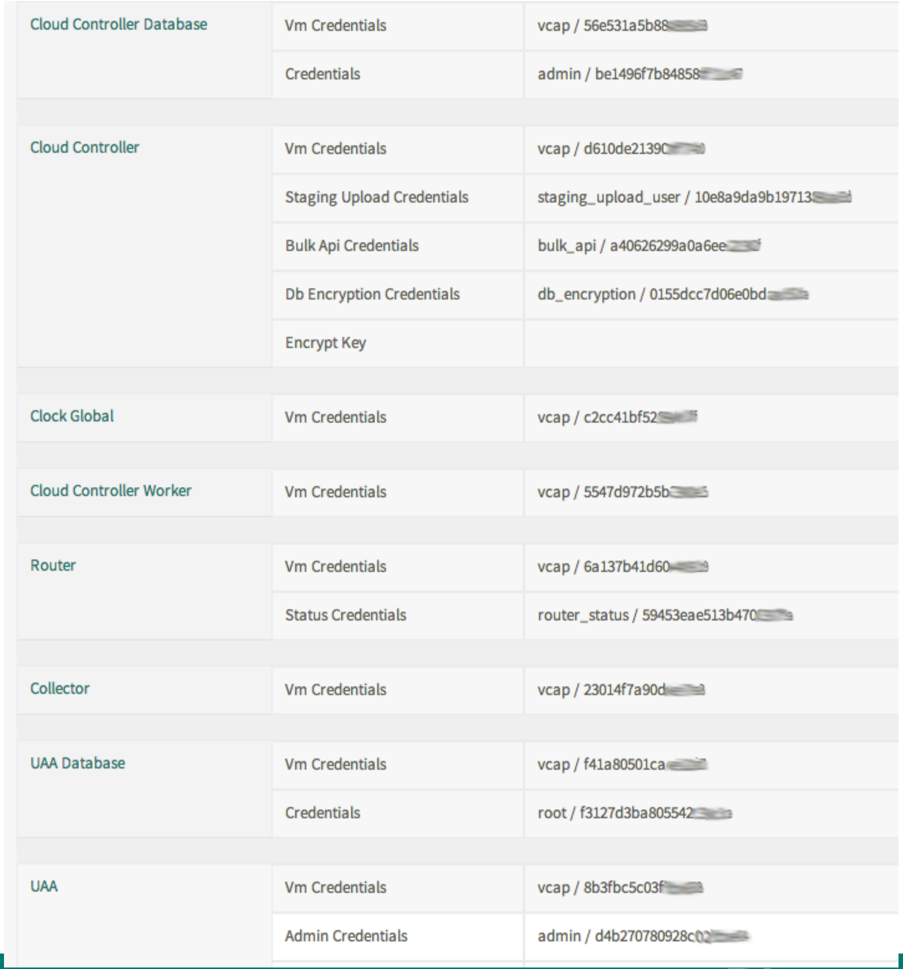
Operations Manager 1.7+ introduces UAA integration for full LDAP/AD/SAML integration



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[redacted]
	Credentials	admin / be1496f7b84858[redacted]
Cloud Controller	Vm Credentials	vcap / d610de2139[redacted]
	Staging Upload Credentials	staging_upload_user / 10e8a9da9b19713[redacted]
	Bulk Api Credentials	bulk_api / a40626299a0a6ee[redacted]
	Db Encryption Credentials	db_encryption / 0155dcc7d06e0bd[redacted]
	Encrypt Key	
Clock Global	Vm Credentials	vcap / c2cc41bf52[redacted]
Cloud Controller Worker	Vm Credentials	vcap / 5547d972b5b[redacted]
Router	Vm Credentials	vcap / 6a137b41d60[redacted]
	Status Credentials	router_status / 59453eae513b470[redacted]
Collector	Vm Credentials	vcap / 23014f7a90d[redacted]
UAA Database	Vm Credentials	vcap / f41a80501ca[redacted]
	Credentials	root / f3127d3ba805542[redacted]
UAA	Vm Credentials	vcap / 8b3fbc5c03f[redacted]
	Admin Credentials	admin / d4b270780928c[redacted]

Multi-tenancy

Overview

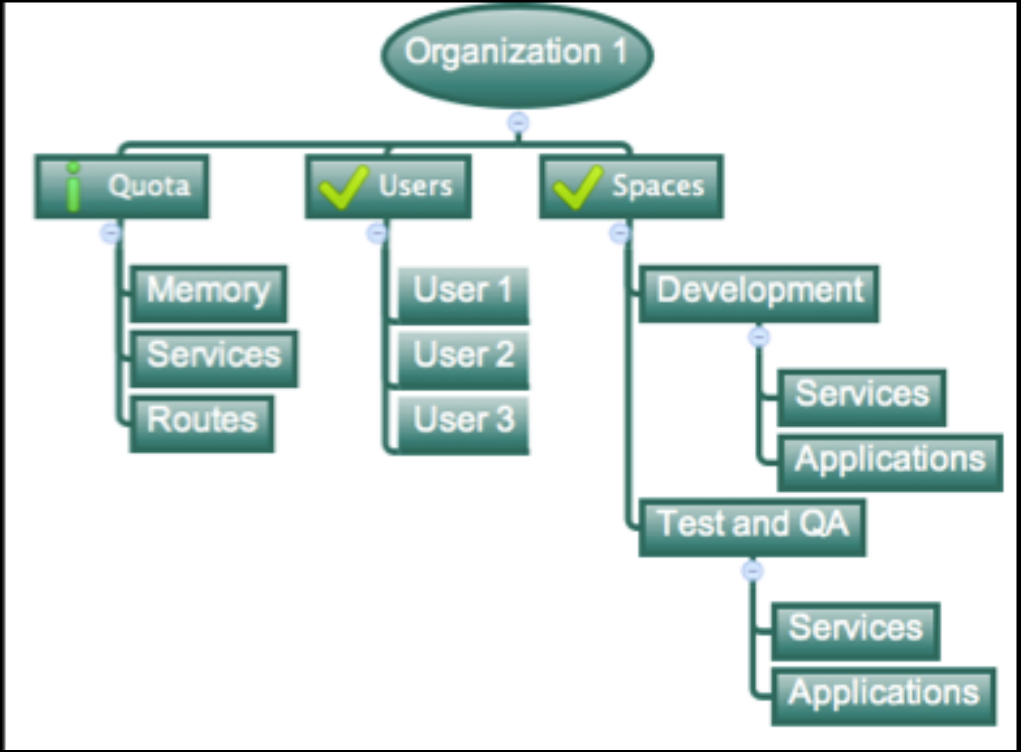
Organizations

Logical division within a Pivotal CF Installation / Foundation.

Each organization has its own users and assigned quota

Sub-divided into Spaces

User permissions / roles are specified per space within an organization



Spaces

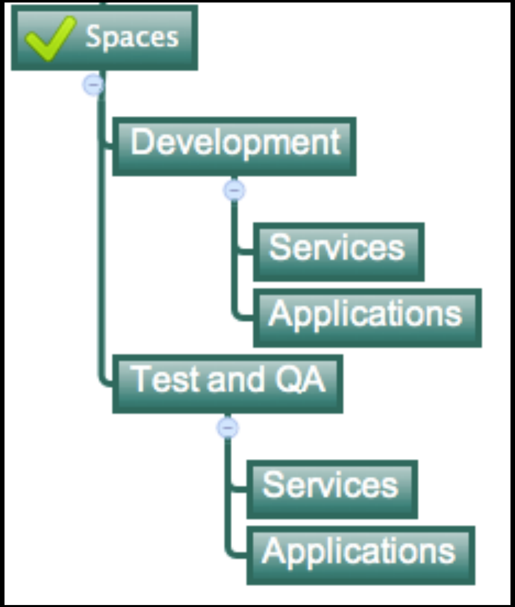
Logical sub-division within an organization

Users authorized at an organization level can have different roles per space

Services and Applications are created / specified per Space

Same Service can have different meanings per space

Spaces can be assigned quotas



Quotas & Plans

Different quota limits (e.g. “small”, “enterprise”, “default”, “runaway”) can be assigned per Org/Space

Quota defines

- Total Memory
- Total # of Services
- Total # of Routes