Pivotal

PCF Operations Workshop – Role Based Access Control

<Presenter>

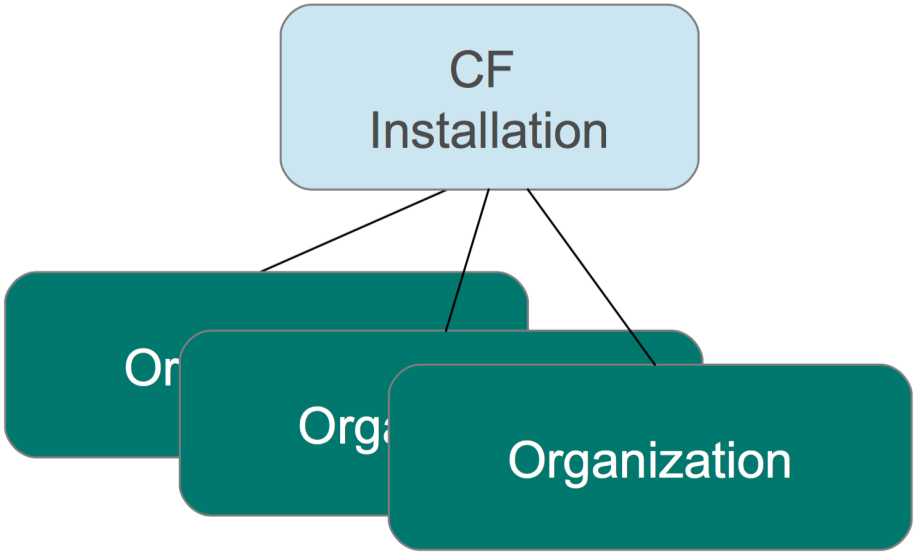
<Title>

Operations Workshop Agenda

- PCF Introduction
- Services Overview
- Platform Installation & Setup
- **Role Based Access Control**
- Platform & Application Scaling
- Platform & Application Health
- Patching & Upgrades
- Authentication and Authorization
- Advanced BOSH

Organizations

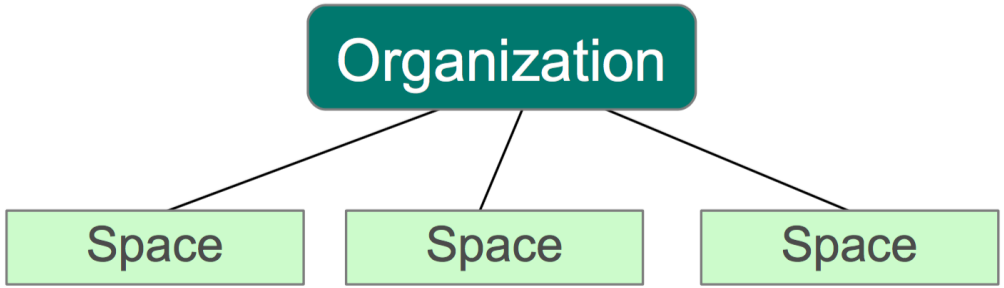
- Top-most administrative unit
- Any Cloud Foundry installation CF
- can have multiple organizations defined in any way
  - A logical way to organize users and resources
  - Typically a company, department, application suite or large project
- Designed to support many users working collaboratively



Spaces

Organizations contains multiple spaces

- Default PWS space: *development*
- Spaces also can be defined in any way
- A logical way to organize users and resources
- For example, *staging* and *production*



Spaces: Applications, Services and Users

- Applications and services are scoped to a space
- Provides a set of users access for:
  - Application development
  - Functionality and/or performance testing
  - Quality assurance
  - Deployment to production
  - Maintenance

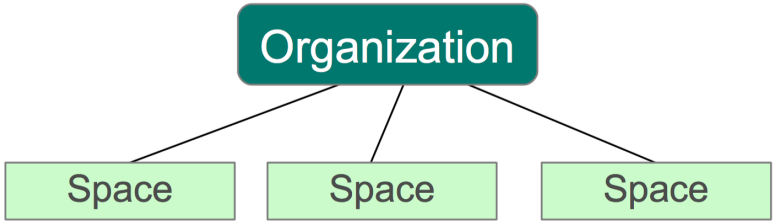
space: *development*

apps: *myApp1, myApp2*
services: *MySQL*
users: *developerA, developerB*

Pivotal

Organizations and Spaces with the cf CLI

- You can use the cf CLI to work with organizations and spaces
- From `$ cf help`



PivotalCloudFoundry_ICM — bash — 95×17

```
ORGS:
   orgs, o                              List all orgs
   org                                  Show org info

   create-org, co                       Create an org
   delete-org                           Delete an org
   rename-org                           Rename an org

SPACES:
   spaces                               List all spaces in an org
   space                                Show space info

   create-space                         Create a space
   delete-space                         Delete a space
   rename-space                         Rename a space
```

Pivotal

Users and Roles

- Users are members of an organization
  - Usually they are operators or developers (not application end users)
  - Users are sent an email invite and asked to create an account
- Users have specific organization and space roles
  - Organization roles grant permissions in an organization
  - Space roles grant permissions in a particular space
  - A combination defines the user's overall permissions

Organization Roles

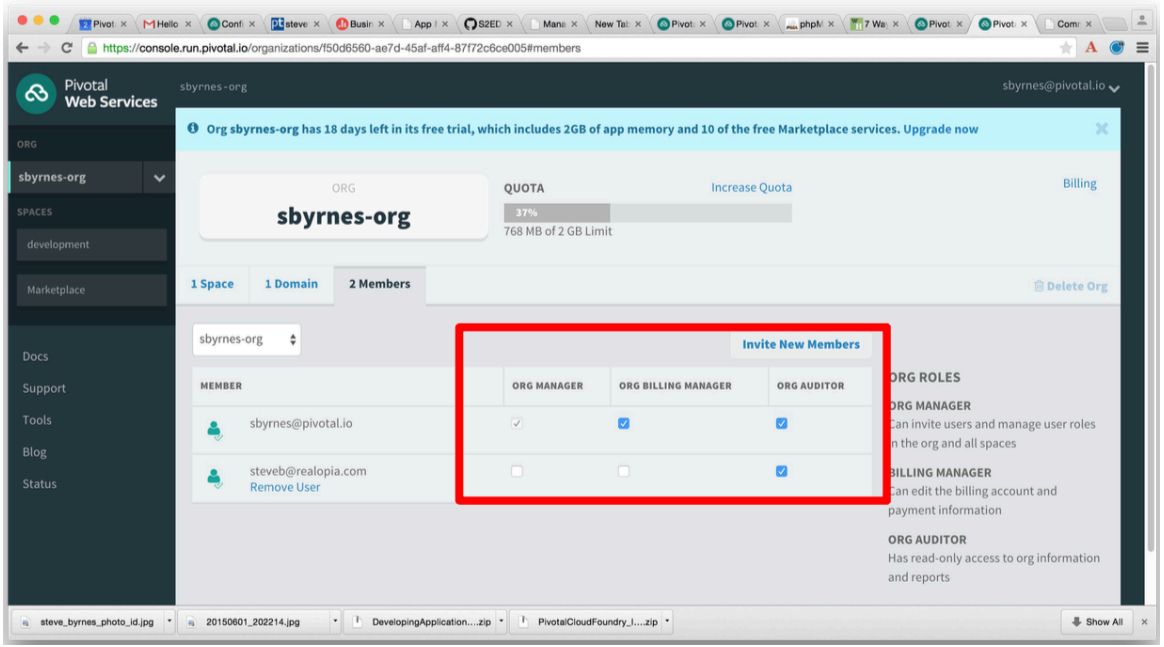
- Organization Manager
  - Can do things like invite/manage users and roles, manage spaces, view application usage Organization Auditor
- Organization Auditor
  - View only access to all org and space info, settings, reports
- Billing Manager
  - Sets org spending limits, and works with invoices and payments
  - Only relevant for Cloud Foundry environments deployed with a billing engine

Space Roles

- Space Manager
  - Can invite/manage users, enable features for a given space
  - Can manage applications and services in a space
- Space Auditor
  - View only access to all space information, settings, reports, logs
- Space Developer
  - Can create, delete, manage applications and services, full access to all usage reports and logs

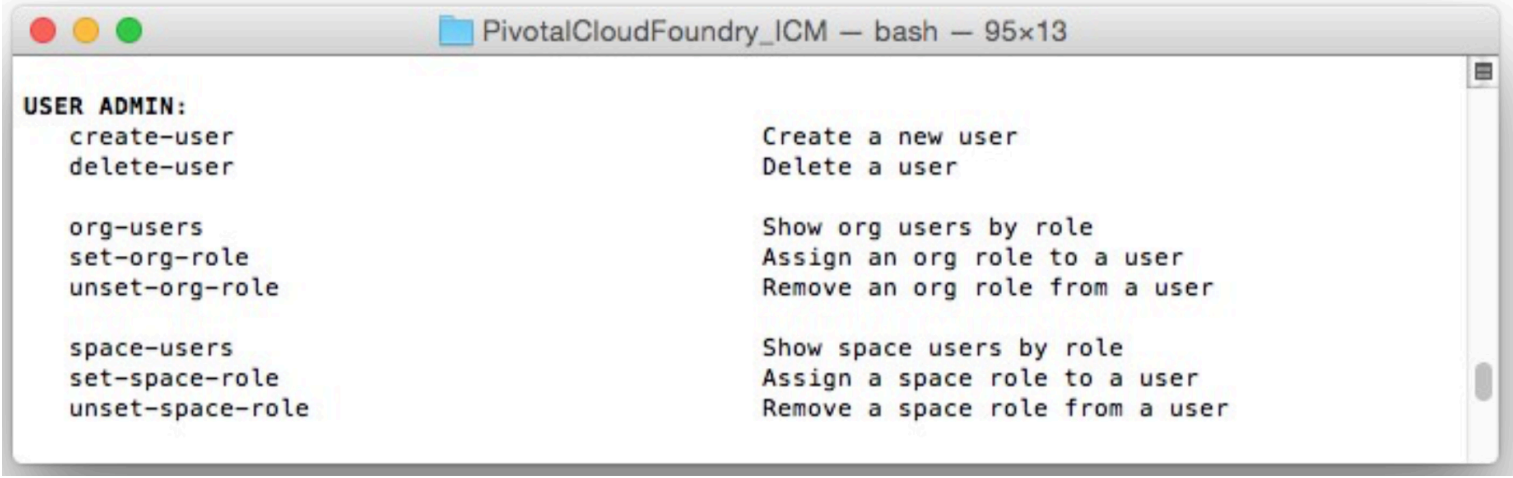
Users and Roles with Apps Manager

- Invite members and assign roles with Apps Manager



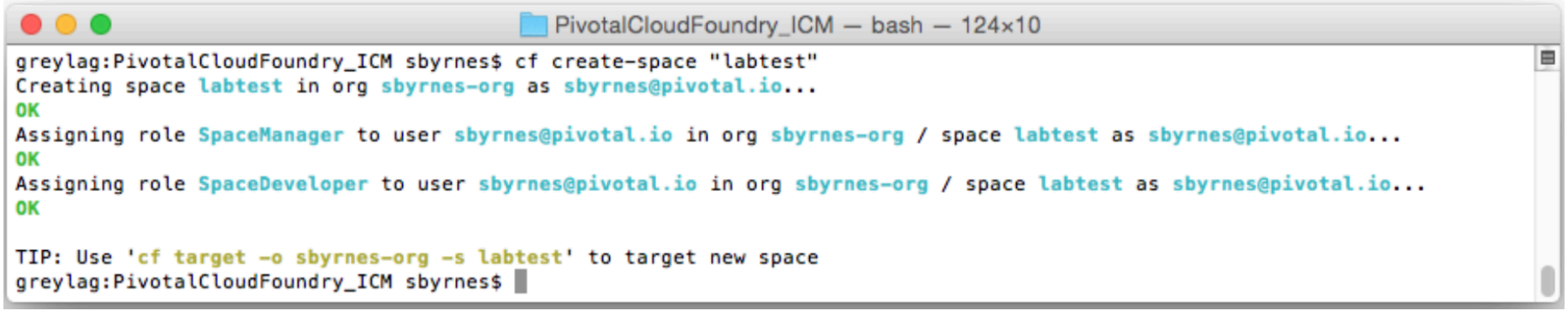
Users and Roles with the CLI

- You can use the cf CLI to work with users and roles
- From `$ cf help`



Roles when Creating a Space

- Creating a space adds new roles for the organization manager in the new space
  - SpaceManager
  - SpaceDeveloper



Pivotal

The Administrator User

- Special Administrator user / role defined
  - Defined for the Cloud Foundry installation
  - Separate from users defined at organization / space
- Several **cf** commands restricted to Administrator only
  - Setting organization and space quotas
  - Defining security groups
  - Administering services
  - Adding, modifying and removing user accounts
- Use without the right role, the cf CLI returns:

```
Server error, status code: 403, error code: 10003, message: You are not
authorized to perform the requested action
```

Pivotal