

The background image is a photograph of the Golden Gate Bridge in San Francisco, California. The bridge is shown from a low angle, looking towards the towers. The sky is overcast and has a dark blue tint, which is reflected in the water below. The towers of the bridge are visible against the sky.

Pivotal

PCF Operations Workshop – Role Based Access Control

Dan Herold – Platform Architect

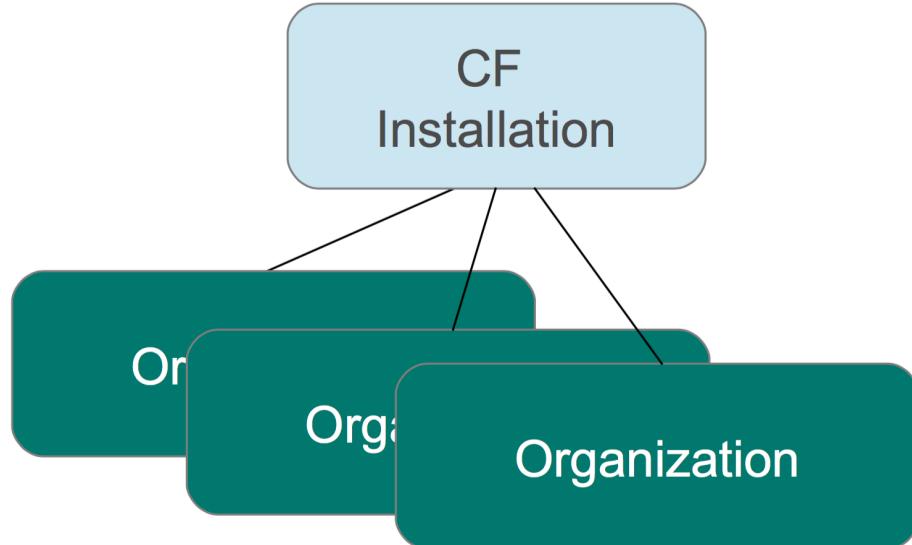
Nenad Momcilovic – Platform Architect

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

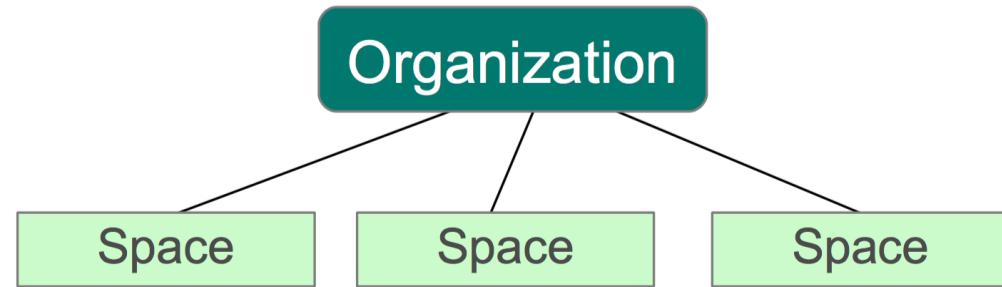
- Top-most administrative unit
- Any Cloud Foundry installation CF
- can have multiple organizations defined in any way
 - A logical way to organize users and resources
 - Typically a company, department, application suite or large project
- Designed to support many users working collaboratively



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

Organizations and Spaces with the cf CLI

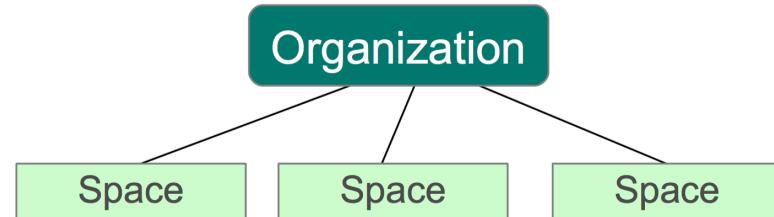
- You can use the cf CLI to work with organizations and spaces
- From `$ cf help`

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

    create-org, co
    delete-org
    rename-org

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

    create-space
    delete-space
    rename-space
```



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

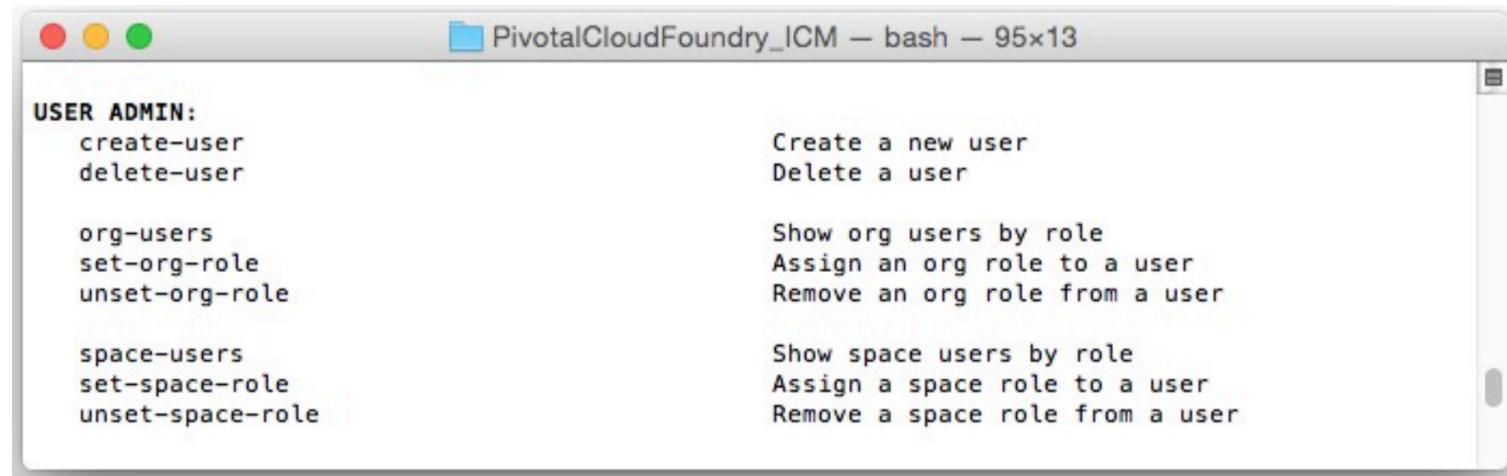
- Invite members and assign roles with Apps Manager

The screenshot shows the Pivotal Web Services Apps Manager interface for the organization 'sbyrnes-org'. The left sidebar includes links for Org, Spaces (development), Marketplace, Docs, Support, Tools, Blog, and Status. The main content area displays the organization summary: 'sbyrnes-org' (1 Space, 1 Domain, 2 Members). It shows a quota of 37% (768 MB of 2 GB Limit) and a link to 'Increase Quota'. A red box highlights the 'Invite New Members' section, which lists two members: 'sbyrnes@pivotal.io' and 'steveb@realopia.com'. For each member, checkboxes are present under 'ORG MANAGER', 'ORG BILLING MANAGER', and 'ORG AUDITOR'. To the right of the members, detailed descriptions of these roles are provided:

- ORG MANAGER**: Can invite users and manage user roles in the org and all spaces.
- BILLING MANAGER**: Can edit the billing account and payment information.
- ORG AUDITOR**: Has read-only access to org information and reports.

Users and Roles with the CLI

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



```
USER ADMIN:
  create-user          Create a new user
  delete-user         Delete a user

  org-users           Show org users by role
  set-org-role        Assign an org role to a user
  unset-org-role     Remove an org role from a user

  space-users         Show space users by role
  set-space-role      Assign a space role to a user
  unset-space-role    Remove a space role from a user
```

Roles when Creating a Space

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



```
greylag:PivotalCloudFoundry_ICM sbyrnes$ cf create-space "labtest"
Creating space labtest in org sbyrnes-org as sbyrnes@pivotal.io...
OK
Assigning role SpaceManager to user sbyrnes@pivotal.io in org sbyrnes-org / space labtest as sbyrnes@pivotal.io...
OK
Assigning role SpaceDeveloper to user sbyrnes@pivotal.io in org sbyrnes-org / space labtest as sbyrnes@pivotal.io...
OK

TIP: Use 'cf target -o sbyrnes-org -s labtest' to target new space
greylag:PivotalCloudFoundry_ICM sbyrnes$
```

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
```