

---

# Building Open Compute Systems using Globus Identity

---

David Champion

GlobusWorld, April 14-15, 2015  
Argonne National Laboratory



THE UNIVERSITY OF  
**CHICAGO**

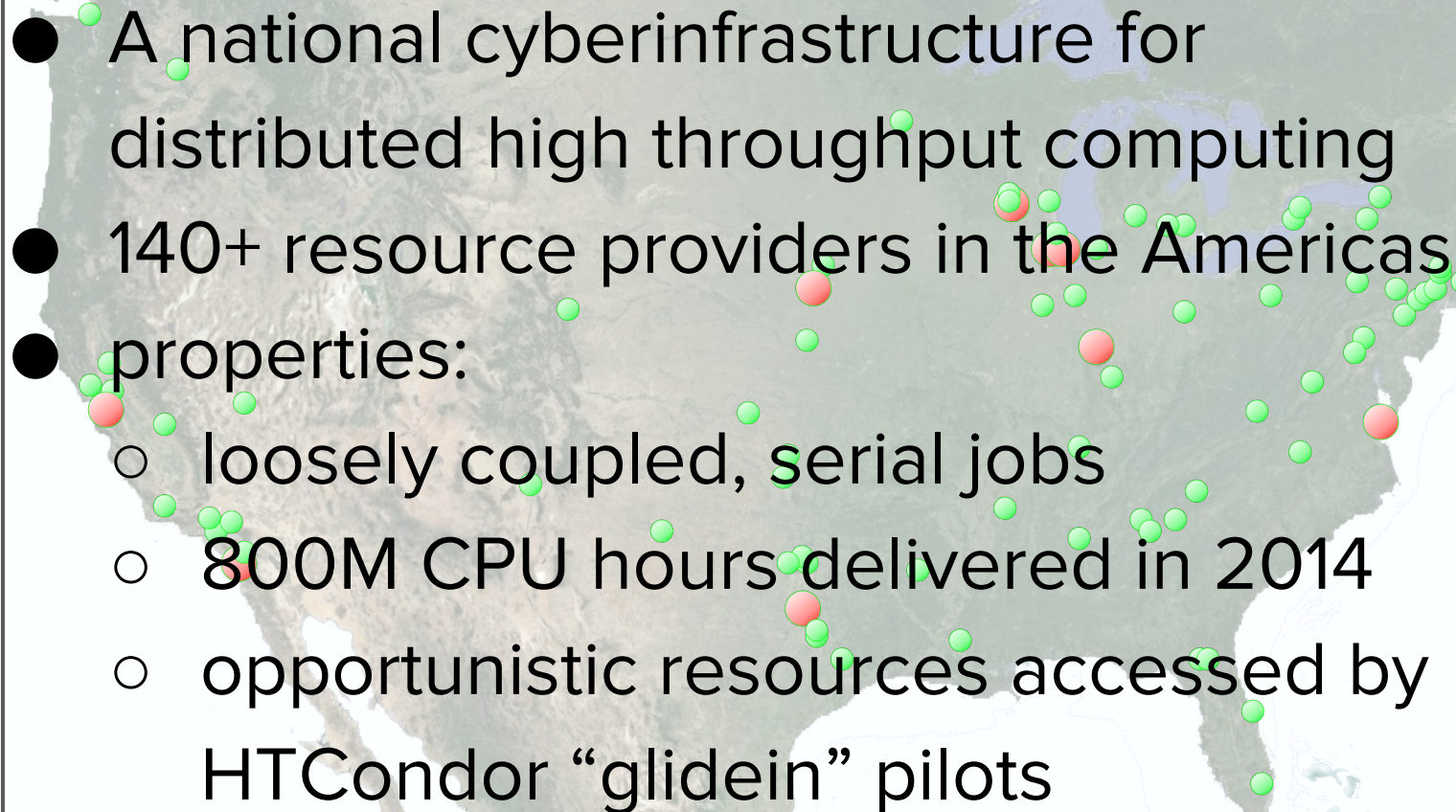


**Open Science Grid**

---

# Open Science Grid

---

- 
- A national cyberinfrastructure for distributed high throughput computing
  - 140+ resource providers in the Americas
  - properties:
    - loosely coupled, serial jobs
    - 800M CPU hours delivered in 2014
    - opportunistic resources accessed by HTCondor “glidein” pilots

# OSG: 140 resource endpoints

---

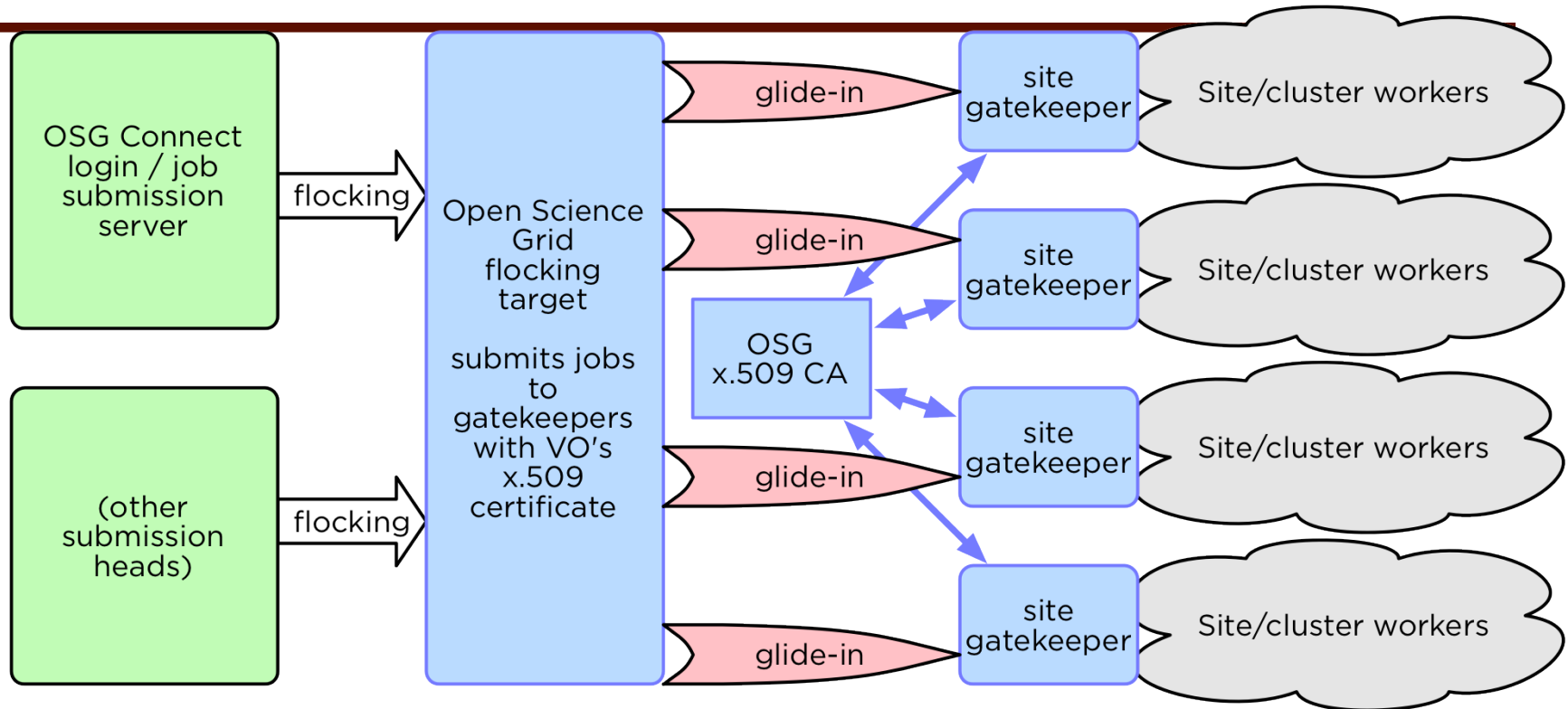
... with campus users far and wide

... with x.509 AuthZ for **virtual organizations**

- Augment with simple sign-up and access for individual researchers
- Use campus identity services
- Reduce time between sign-up and job submission

→ **OSG Connect**

# OSG VO high-level architecture



~ 10 submission sites

one flocking target

gk+cluster for each site (~140)

- x.509 virtual organization validation occurs during wide area job distribution.
- **trust relationship** between the resource provider and the OSG VO.
- **users not required to use x.509 certificates directly.**

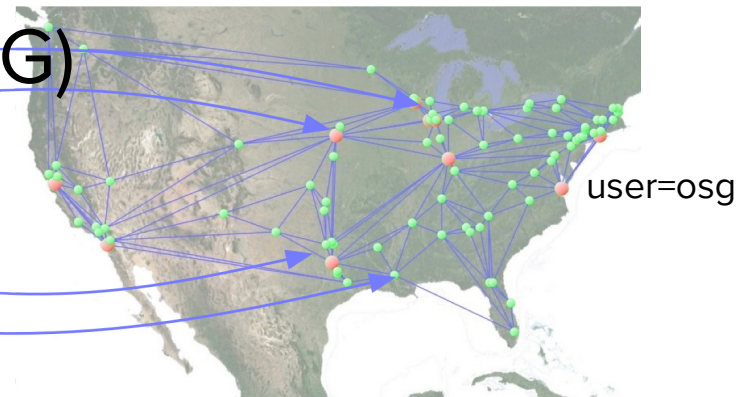


# OSG Connect

---

- A central entry point for campus-based users and individual PI's
- Access to resources using the OSG VO and glidein service
- An *identity bridge*: campus identity (CILogon) ▶ OSG Connect identity (Globus) ▶ virtual organization roles (OSG)

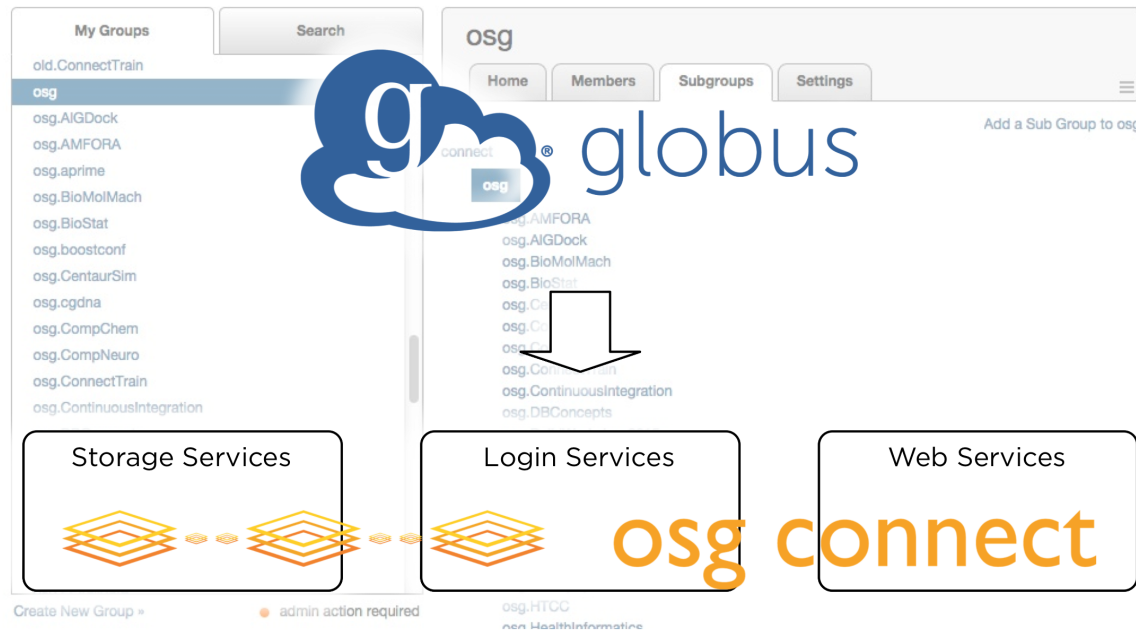
user=angus  
user=bobby  
user=carol  
user=donna  
user=eddie



# Establishing identity

---

- How do we get from <campus researcher> to user=angus on OSG Connect?
  - Globus Nexus provides an answer.



# IdM with Nexus

The screenshot displays the IdM user interface. On the left, a sidebar lists various groups under 'My Groups'. The main content area shows the 'osg.AIGDock' group page, which includes tabs for 'Home', 'Members', 'Subgroups', and 'Settings'. The 'Members' tab is active, showing a list of group members with columns for name, email, username, and member since. A red circle highlights the entry for 'David Minh' with email 'dminh@iit.edu' and username 'daveminh'. Below the active members, there is a 'Rejected' section with a table of users who have been rejected from the group. A red circle highlights the 'Change Password' button in the navigation bar. Below the navigation bar, the 'Manage Identities' section is visible, showing a table of linked identities. A red circle highlights the entry 'ssh2 - dgc@laptop' with type 'SSH' and provider 'ssh authorized key'. A red callout box on the right side of the image contains the text 'Customer-directed team management'. Another red callout box on the left side contains the text 'Self-service profile and credential control'. A third red callout box at the bottom left contains the text 'SSH key upload (for login shell)'.

My Groups Search

osg.AIGDock

Home Members Subgroups Settings

7 active 1 rejected

Invite people to this group

Active Members

name	email	username	member since
CI Connect	accounts@ci-connect.net	connect	a year ago
David Minh	dminh@iit.edu	daveminh	a year ago
OSG Connect Sp...	accounts@osgconnect...	osgconnect	10 months ago
Bing Xie	bxie4@hawk.iit.edu	bxie	8 months ago
Chen Li	cli78@hawk.iit.edu	jesseleechen	8 months ago
Laurentiu Spiridon	lspirido@iit.edu	spirilaurentiu	8 months ago
Trung Hai Nguyen	trnguye46@iit.edu	nguyentrung	3 months ago

Rejected

name	email	username	status changed
Administrator	support@ci-connect.net	osgconnectadmin	10 months ago

Update Profile Change Password Account Privacy Globus Plus Manage Identities

Manage Identities + add linked identity

label	type	provider
SSO: Google <dgc@example.org>	OpenID	google.com
ssh2 - dgc@laptop	SSH	ssh authorized key
OSG OIM DigiCert	X.509	X.509 certificate
x509 - tutorial	X.509	X.509 certificate

Customer-directed team management

Self-service profile and credential control

SSH key upload (for login shell)

# Python Nexus Client

---

- Nexus exposes a REST Web Service (API)
  - Globus provides Nexus API client for Python
    - <https://github.com/globusonline/python-nexus-client>
  - Using the API, we:
    - search our group hierarchy for relevant changes
    - store these changes locally to track current state
    - provision user accounts into directory (nss\_nis)
    - provision user filestores into storage systems
    - populate local group space as a pure reflection of Nexus groups
    - define access rights to GridFTP and job submission
-



# Python Nexus Client (example)

---

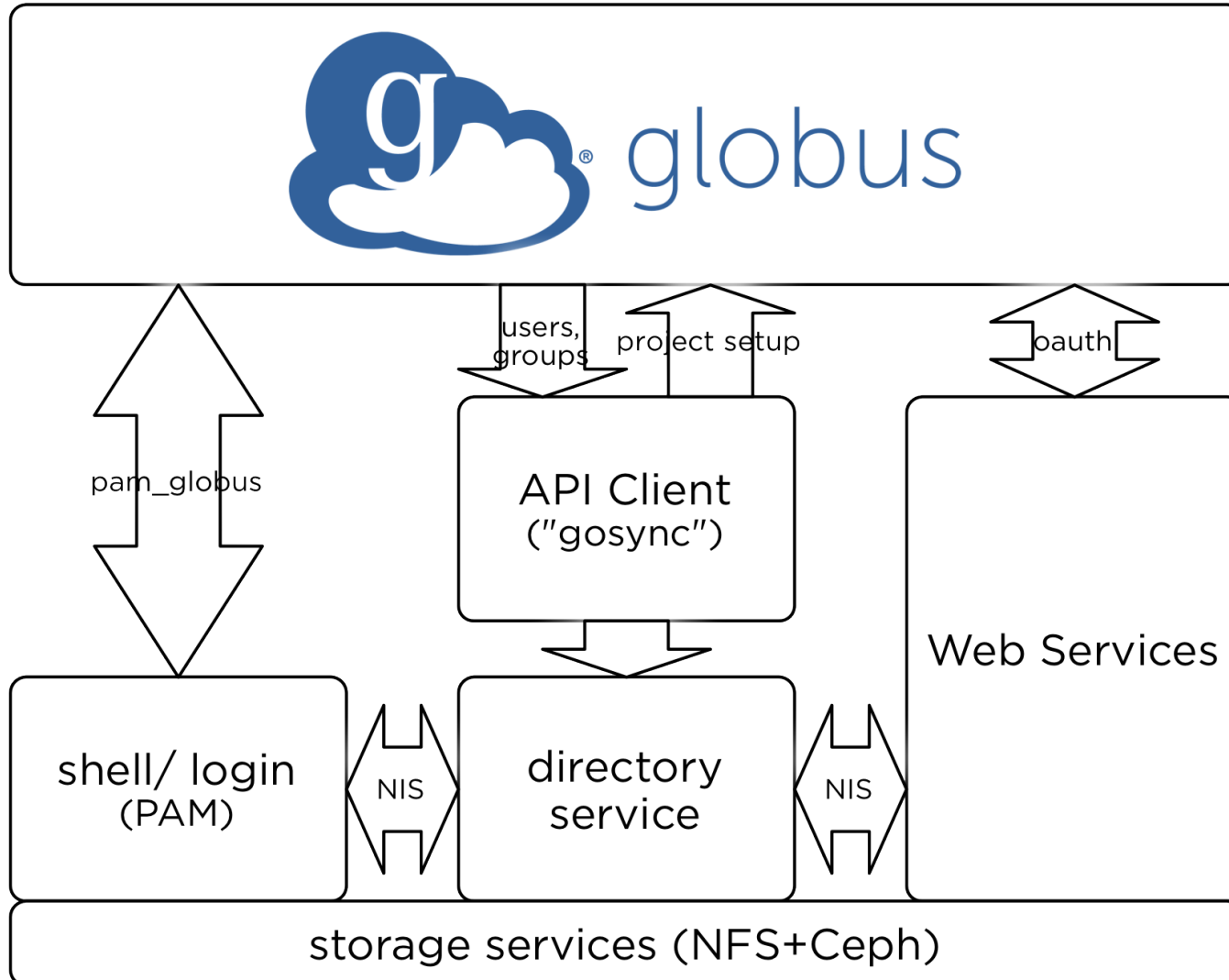
```
from nexus import GlobusOnlineRestClient

config = {
    'server': 'nexus.api.globusonline.org',
    'client': 'osgconnect',      # service account
    'client_secret': 'password', # secret!
}

gc = GlobusOnlineRestClient(config=config)
headers, response = gc.get_group_members(groupuuid)
members = response['members']
members = [member for member in members if member and member['username']]
members.sort(lambda a, b: cmp(a['status'], b['status']) or cmp(a['username'], b['username']))
for member in members:
    print '%s (%s) %s' % (group, member['status'], member['username'])
    headers, profile = gc.get_user_profile(member['username'])
    if profile.has_key('credentials'):
        keys = sorted([cred['ssh_key'] for cred in prof['credentials'] if cred['credential_type'] ==
'ssh2'])
        # store ssh keys into ~/.authorized_keys
```

---

# Summary: Data flow architecture



- OSG Connect
- ~340 users
  - ~60 projects
  - ~40 campuses

Architecture extended to other campus integrations via **CI Connect:**

ATLAS  
CMS  
Duke University  
UChicago

# Thank you!

---

And our thanks to the Globus, CILogon and OSG teams. In particular:

- Rachana Ananthakrishnan (Globus)
  - Mattias Lidman (Globus)
  - Stephen Rosen (Globus)
  - Mats Rynge (OSG)
  - Jim Basney (CILogon) and the InCommon federation
-

# Further information

---

Open Science Grid

<http://opensciencegrid.org/>

OSG Connect

<http://osgconnect.net/>

Python Nexus Client

<https://github.com/globusonline/python-nexus-client>

---