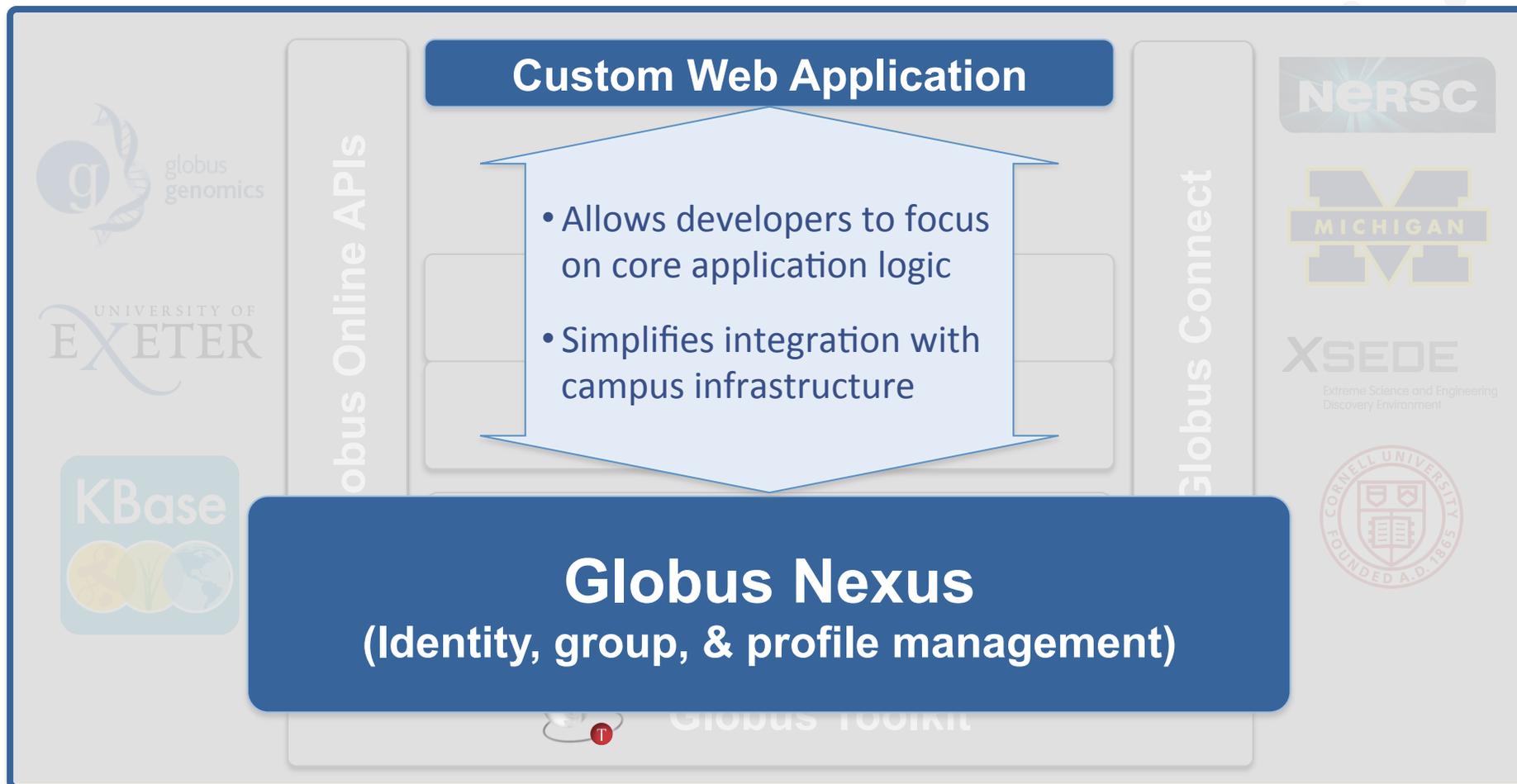


# The identity challenge in science



- Developers of collaborative science tools, applications, and cyberinfrastructures need to:
  - **Assign identities** to their users
  - Manage **user profiles**
  - Organize users into **groups** for authorization
- Providing **high-quality implementations** of such capabilities is challenging
  - Complexity of associated security protocols
  - Reliability, availability, scalability, security are all hard
- The result is **many identity ‘islands’** across science domains and projects—often poorly implemented

# Streamline collaborative tool development

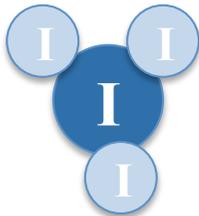


# Nexus provides four key capabilities



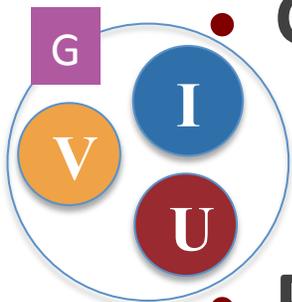
## Identity provisioning

- Create and manage Globus identities



## Identity hub

- Link with other identities; use to authenticate to Nexus and other services



## Group hub

- User-managed group creation, management; groups can be used for authorization

## Profile management



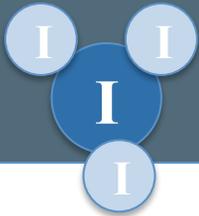
- User-managed profile attributes and visibility; can be used in group admission

# I Identity provisioning



- Globus Nexus can act as an identity provider (IDP) for a project
  - User management, email validation...
- DOE Systems Biology Knowledge Base (kBase) is an example of such a project. ~400 identities to date

The screenshot shows the KBase Predictive Biology DOE Systems Biology Knowledgebase website. At the top left is the KBase logo with three circular icons (a yellow one with a DNA helix, a green one with a plant, and a blue one with a globe). Below the logo is the text "KBase PREDICTIVE BIOLOGY" and "DOE Systems Biology Knowledgebase". A dark navigation bar contains a "Log In" button and a "Sign Up" button. Below the navigation bar, the text "Sign Up..." is displayed on the left, and "Already a member? [Sign In.](#)" is on the right. A paragraph of text states: "KBase has partnered with Globus Online to provide a single account and group management system for applications across KBase." Below this text are three input fields labeled "Full Name", "Email", and "Username".



# Identity hub



- **Link identities** from other federated IDP(s) with a Nexus identity
  - E.g., InCommon (SAML), Google (OpenID), XSEDE (OAuth MyProxy), IGTF-certified X.509 CA, SSH
- **Use linked identity** to authenticate to Nexus as the Nexus identity (e.g., use campus identity)
- **Leverage Nexus federated IDP** to 3rd-party services
  - Via Oauth or LDAP
  - E.g., to XSEDE, Jira, Zendesk, Drupal, Globus data management, Confluence
- Have Nexus **cache delegated credentials**
  - X.509, via CILogon, MyProxy

# Identity hub management



Manage Data | Groups | Support | **ian**

[update profile](#) | [change password](#) | [account privacy](#) | [group membership](#) | [manage identities](#) | [log out](#)

## Manage Identities

[Add External Identity](#) | [Add X.509 Certificate](#) | [Add SSH Public Key](#)

Alias	Type	Authentication Provider			
system-generated openid alias	openid	google.com	<a href="#">View Details</a>	<a href="#">Update</a>	<a href="#">Delete</a>
CI	myproxy	grid.ci.uchicago.edu	<a href="#">View Details</a>	<a href="#">Update</a>	<a href="#">Delete</a>
	myproxy	dev.esg.anl.gov:7512	<a href="#">View Details</a>	<a href="#">Update</a>	<a href="#">Delete</a>
MBook	ssh2	SSH Public Key	<a href="#">View Details</a>	<a href="#">Update</a>	<a href="#">Delete</a>
galaxy-climate	x509	/O=Grid/OU=DemoG.			<a href="#">Delete</a>
Ian Laptop	x509	/C=US/O=Globus C...			<a href="#">Delete</a>
InCommon / CILogon Sign In	oauth	cilogon.org			<a href="#">Delete</a>

[Add External Identity](#) | [Add X.509](#)

### Add External Identity

**Alias**

**Account Provider**

InCommon / CILogon

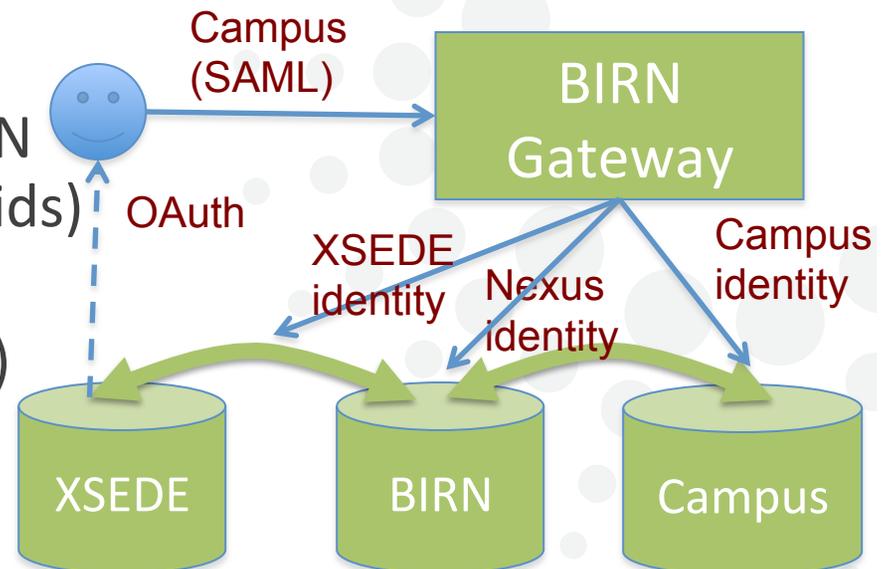
[Add Account](#) [Close](#)

# Identity hub: Biomedical science



- Dr. Smith creates a BIRN id (Nexus id via BIRN-tailored interface)
- Dr. Smith links campus id and XSEDE id
- Dr. Smith can then:
  - Authenticate to BIRN with campus id
  - Query catalog (Nexus/BIRN id)
  - Request data transfer from BIRN to campus (Nexus and campus ids)
  - Request transfer from BIRN to XSEDE (Nexus and XSEDE ids)
  - Repeat these tasks: use cached credentials

Name: Dr. Smith  
Email: smith@u.edu  
Linked id: Campus  
Linked id: XSEDE



(BIRN=Biomedical Informatics Research Network)

# Use linked identity



Sign In

Select a different login

GlobusOnline	InCommon / CILogon
Argonne LCF	LRZ
Argonne MCS & LCRC	NCSA
BIRN	NCSA Blue Waters
CLI Transition	NERSC
EGI	UChicago CI
ESG ANL	UChicago iBi
Exeter	UK NGS
Google	westGrid
	<b>XSEDE</b>

Sign In

Use Your XSEDE login

[alternate log](#)

You will now be redirected to XSEDE's authentication page.

Proceed

XSEDE User Portal Delegation

https://portal.xsede.org/oauth/authorize?oauth\_token=myproxy%3Aoa4mp%2C2012%3A%2FtempCred%2F646a304b65...

## XSEDE

Extreme Science and Engineering  
Discovery Environment

Welcome to the XSEDE User Portal Authorization Page

Science Gateway Access

The XSEDE Science Gateway or Service below is requesting access to your XSEDE account. If you approve, please sign in with your XSEDE username and password.

Note: Only members of active XSEDE project allocations will be able to sign in on this page.

SCIENCE GATEWAY INFORMATION	SIGN IN
The XSEDE Science Gateway listed below is requesting access to your XSEDE account. If you approve, please sign in.	Username: demodoc
Name: Globus Online URL: https://www.globusonline.org/	Password: .....
	<input type="button" value="SIGN IN"/> <input type="button" value="CANCEL"/>

Please send any questions or comments about this site to [help@xsede.org](mailto:help@xsede.org).



# Group hub



- User-managed group creation, management
- Flexible control over admission policies and visibility
- Groups can be used in authorization decisions

## Example: kBase

- Every kBase user added to **kbase\_users**
- Subgroups also created
- Groups used for access control

The screenshot shows a user interface for a group management system. At the top, there is a navigation bar with links for 'Dashboard', 'Groups', 'ian's account', and 'Log Out'. Below this, the main content area is divided into two columns. The left column is titled 'My Groups' and shows a list of groups, with 'kbase\_users' highlighted. Below this, a box titled 'kbase\_users' contains three buttons: 'Home', 'Members', and 'SubGroups'. Underneath these buttons, a list of subgroups is shown: 'kbase\_staff', 'kbase\_microbes', and 'ENIGMA'. The right column contains three main sections: 'Browse Groups' (with a description 'Browse and join groups'), 'My Account' (with a description 'View and change your account settings, including contact information and security credentials'), and 'KBase Site' (with a description 'Return to the main KBase website').

# Group membership interface



## Group Membership

Group Name	Status	
Cornell demo	Pending Admin Approval	✕
Data Summit Slides	Administrator	✕
Globus Team	Active Member	✕
Ian's secret stuff group	Administrator	✕
Ag-GRID	Active Member	✕

### Kyle's Group

Home Members SubGroups Settings

1 active 2 invited 1 rejected

[+ Invite people to this group](#)

### Invitation Sent - Awaiting Response

name	email	username	request sent
-	chard@uchicago.edu	-	today
josh	josh.bryan@gmail.com	jbryan	today

### Active Members

name	email	username	member since
Kyle Chard	kyle@ci.uchicago.edu	kyle	today

### Kyle's Group

Home Members SubGroups Settings

Policies Membership Fields Advanced

edit

**Group is visible to** logged in users (visible to all Globus Online members).

**Member names are visible to** this group's administrators only.

**Subgroups for this group may be created by** admins only

**Users may request membership if they are** invited to join this group.

**Membership requests are approved** automatically for invitations sent by admins & managers

# Branded sites



BLUE WATERS  
SUSTAINED PETASCALE COMPUTING

Reliable, high-performance, secure file transfer by Globus Online.

Blue Waters has partnered with the Globus Online file transfer service.

You may access this service by entering your Blue Waters username and password.

Sign In

Use Your NCSA Blue Waters login alternate login

NOTE: If you are accessing this file transfer service for the first time, you will be redirected to the NCSA Blue Waters authentication page.

Proceed

**XSEDE**

osg connect

Support Resources OSG Connect Sign In / Register

Efficiently connect your science to cycles and data

osg connect

Sign In Sign Up with Globus Online

Using your InCommon / CILogon login alternate login

You will now be redirected to InCommon / CILogon's authentication page.

Proceed

**Open Science Grid**

Research Computing Center

Log In Sign Up

Sign In

Use Your InCommon / CILogon login alternate login

You will now be redirected to InCommon / CILogon's authentication page.

Proceed

**University of Chicago**

KBase  
DOE Systems Biology Knowledgebase

Log In Sign Up

Sign In Sign Up with Globus Online

Use Your GlobusOnline login alternate login

Username Password

Sign In Forgot Password?

**DOE kBase**

U.S. DEPARTMENT OF ENERGY Office of Science

KBase is sponsored by the U.S. Department of Energy's Office of Biological and Environmental Research.

Privacy and Security Notice

INDIANA UNIVERSITY Cyberinfrastructure Gateway

Sign In

Sign In

Use Your InCommon / CILogon login alternate login

You will now be redirected to InCommon / CILogon's authentication page.

Proceed

**Indiana University**

UNIVERSITY OF EXETER

Sign In

Use Your Exeter login alternate login

You will now be redirected to Exeter's authentication page.

Proceed

**University of Exeter**

globus online

Sign In

Use Your EG login alternate login

You will now be redirected to EG's authentication page.

Proceed

**Globus Online**

NERSC

Sign In

Sign In

Use Your NERSC login alternate login

Username Password

Sign In

**NERSC**

BIRN ACCESS Group Management

Sign In

ACCESS is a user and group management system used by the BIRN community to allow editing access to the BIRN WGL.

Sign in with your Globus Online ID.

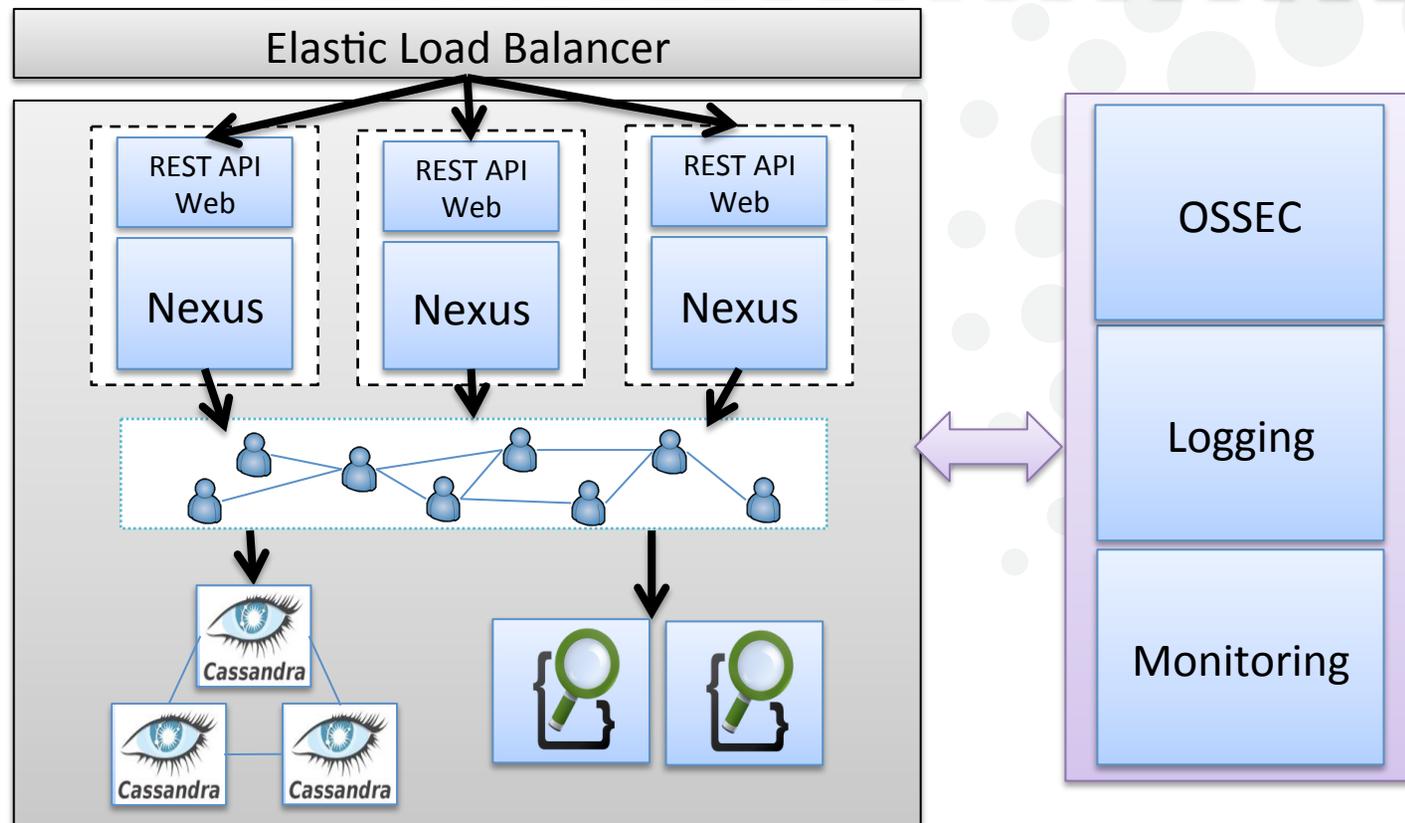
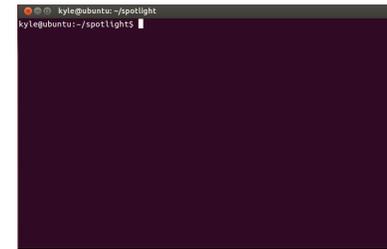
Are you working with a BIRN Working Group or user community and need editing access to the BIRN WGL? Sign up here.

Username Password

Sign In

**NIH BIRN**

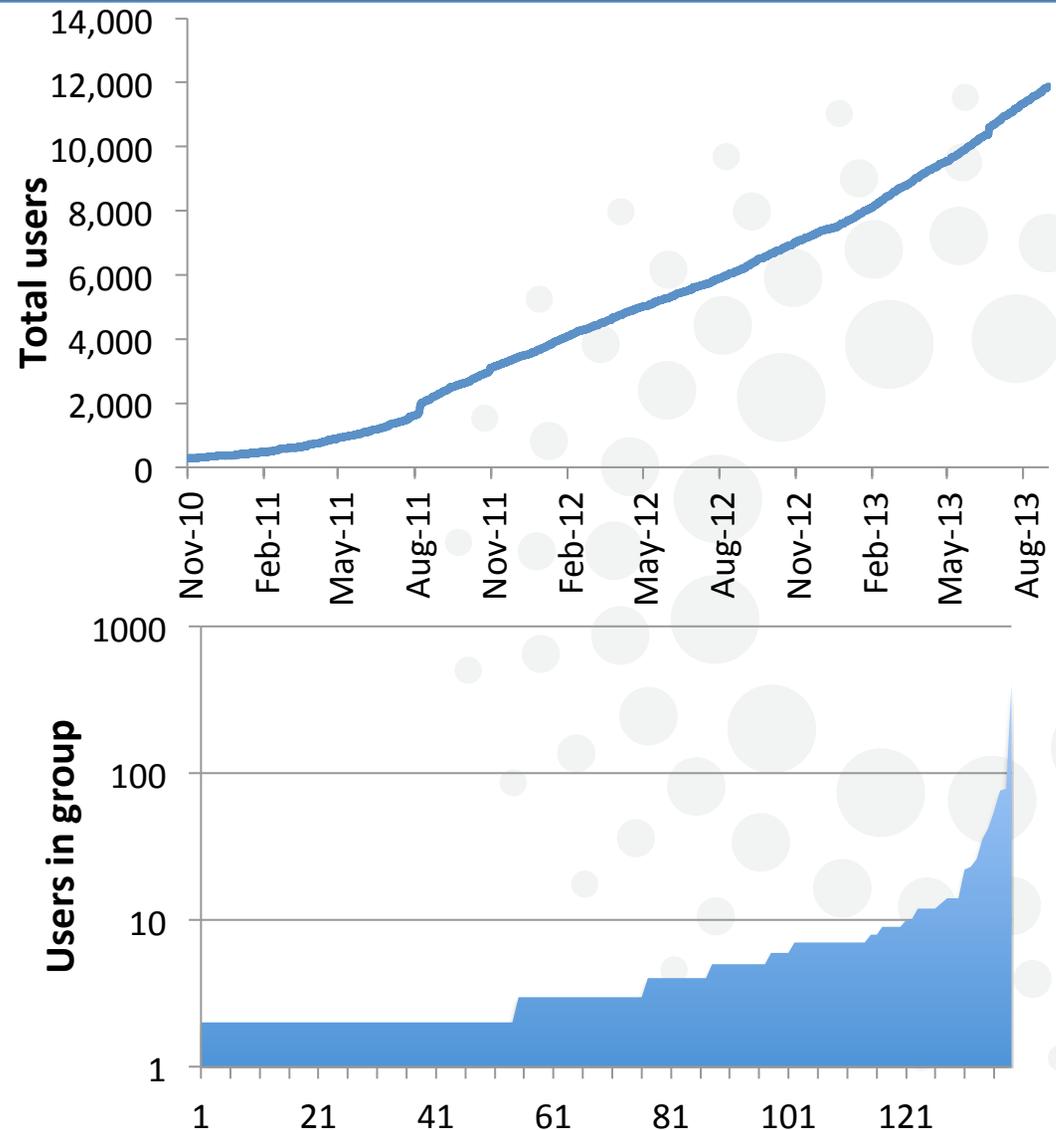
# Implementation and deployment



# Globus Nexus usage as of 9/13



- **>12,000** users and **4977** linked identities
- **557** groups totaling:
  - **1638** active members
  - **229** pending or invited members
  - **162** rejected or suspended members
- Largest group (kbase) has **402** members



# User profiles



- Profile = set of attributes/values about a user
  - E.g., name, email, address, field of science, etc.
- Types of profile attributes:
  - Self-asserted (e.g., name)
  - Validated (e.g., email, linked identity)
  - Asserted by other user
- Sources of profile attributes:
  - Social sites (e.g., LinkedIn, Facebook, Google+)
  - Campus Shibboleth servers
  - Nexus users

# Identities and groups in XSEDE



- Proposal: Replace current ad-hoc systems with Globus Nexus identity and group service
  - Reduce complexity, reduce cost, increase capability
- Careful process of documentation and review
  - “Architecture and development requirements: User and identity management”
  - “User management proposal: Affected use cases”
  - “User management proposal: Motivating stories”
  - “Proposal: Refactoring XSEDE identity and group capabilities”
- Hope to reach closure by end of 2013