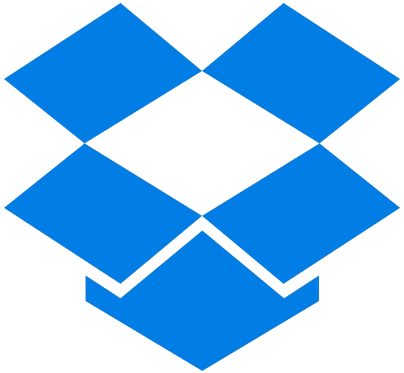


Merou

A decentralised audit framework

Luke Faraone
Dropbox

What is it?

authorisation service

open source

decentralised

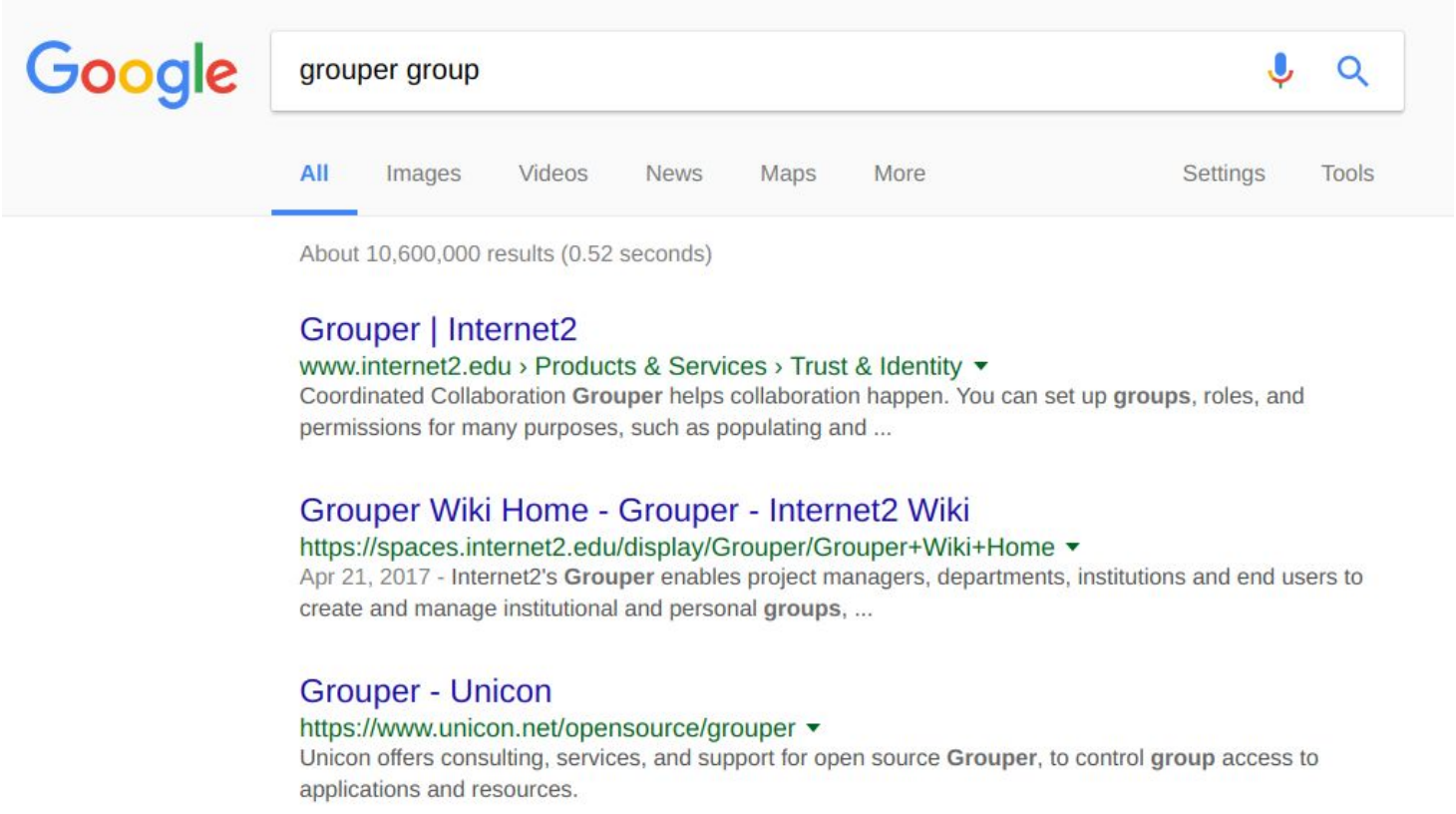
audited



Before we continue...

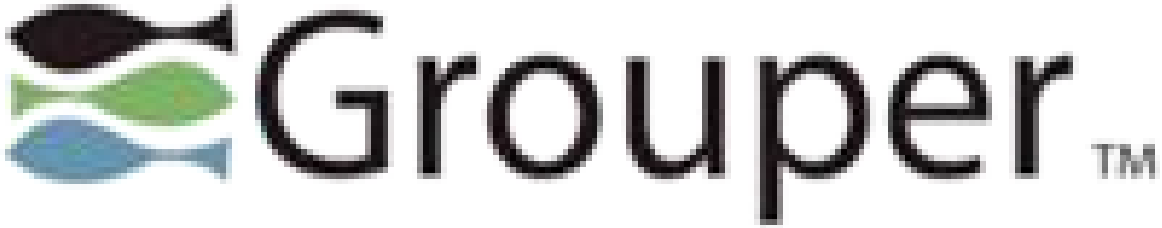


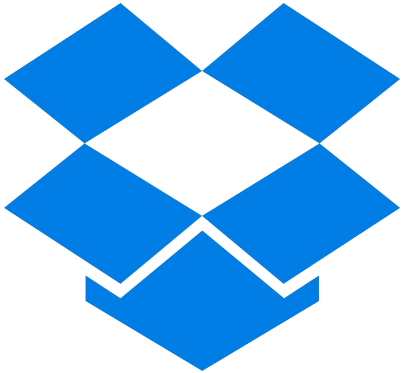
Interns, man.


Google
grouper group
All
Images
Videos
News
Maps
More
Settings
Tools
About 10,600,000 results (0.52 seconds)
Grouper | Internet2
www.internet2.edu › Products & Services › Trust & Identity
Coordinated Collaboration Grouper helps collaboration happen. You can set up groups, roles, and permissions for many purposes, such as populating and ...
Grouper Wiki Home - Grouper - Internet2 Wiki
https://spaces.internet2.edu/display/Grouper/Grouper+Wiki+Home
Apr 21, 2017 - Internet2's Grouper enables project managers, departments, institutions and end users to create and manage institutional and personal groups, ...
Grouper - Unicon
https://www.unicon.net/opensource/grouper
Unicon offers consulting, services, and support for open source Grouper, to control group access to applications and resources.

Naming is hard







~~Grouper~~ Merou

A decentralised audit framework

Luke Faraone
Dropbox

Why does it matter?

Granularity

Usable software means users won't hate interacting with it.

Scalability

Reduces choke-points, removes central teams from the critical path

Visibility

Membership and access control are all in one place

Why does it matter?

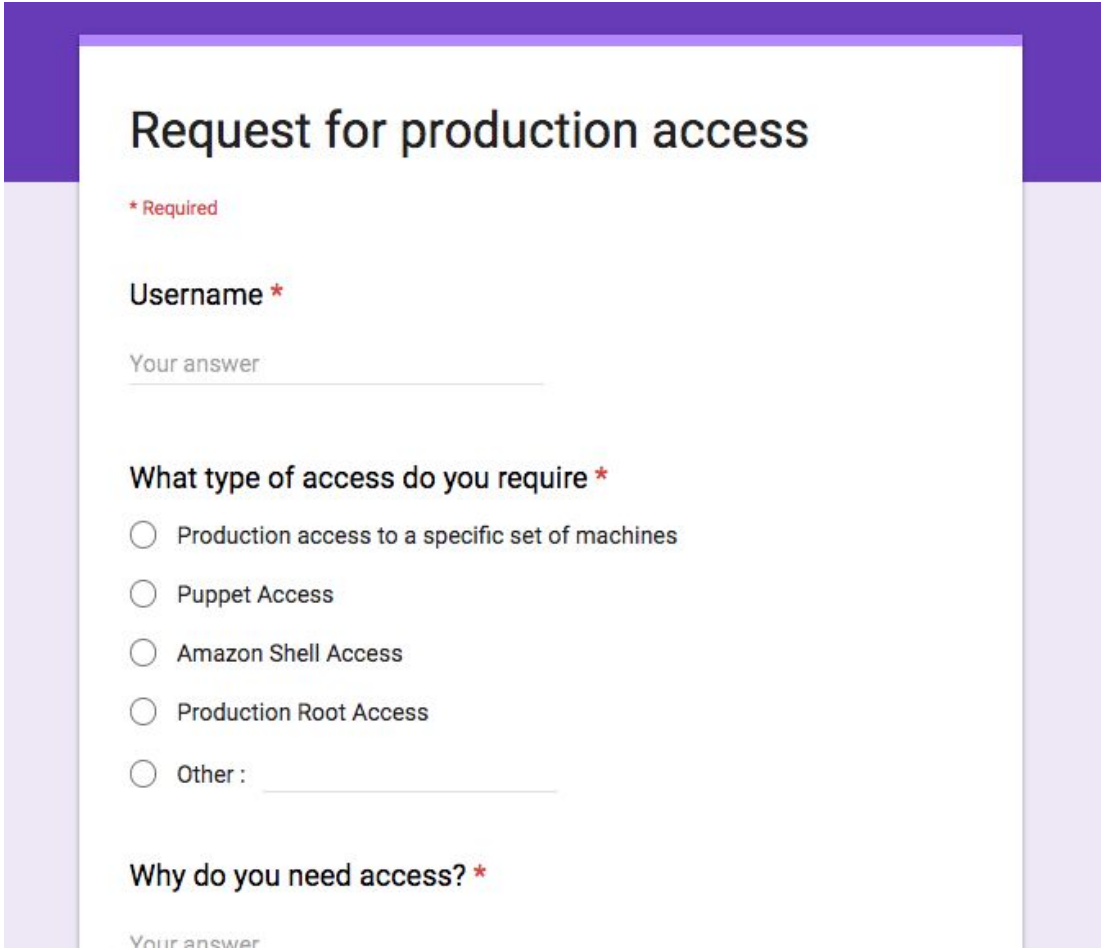


"Who gave a sales engineer access to prod?!"



"OK, fine, we'll implement a process"

In the beginning...



Request for production access

* Required

Username *

Your answer

What type of access do you require *

- ○ Production access to a specific set of machines
- ○ Puppet Access
- ○ Amazon Shell Access
- ○ Production Root Access
- ○ Other :

Why do you need access? *

Your answer

Which, quickly we realised...

Effort

Approval and actioning tracked manually

SPOF

Small number of approvers / actioners



Which, quickly we realised...

Automation???

What, are we going to write Google Apps Script?

Truth?

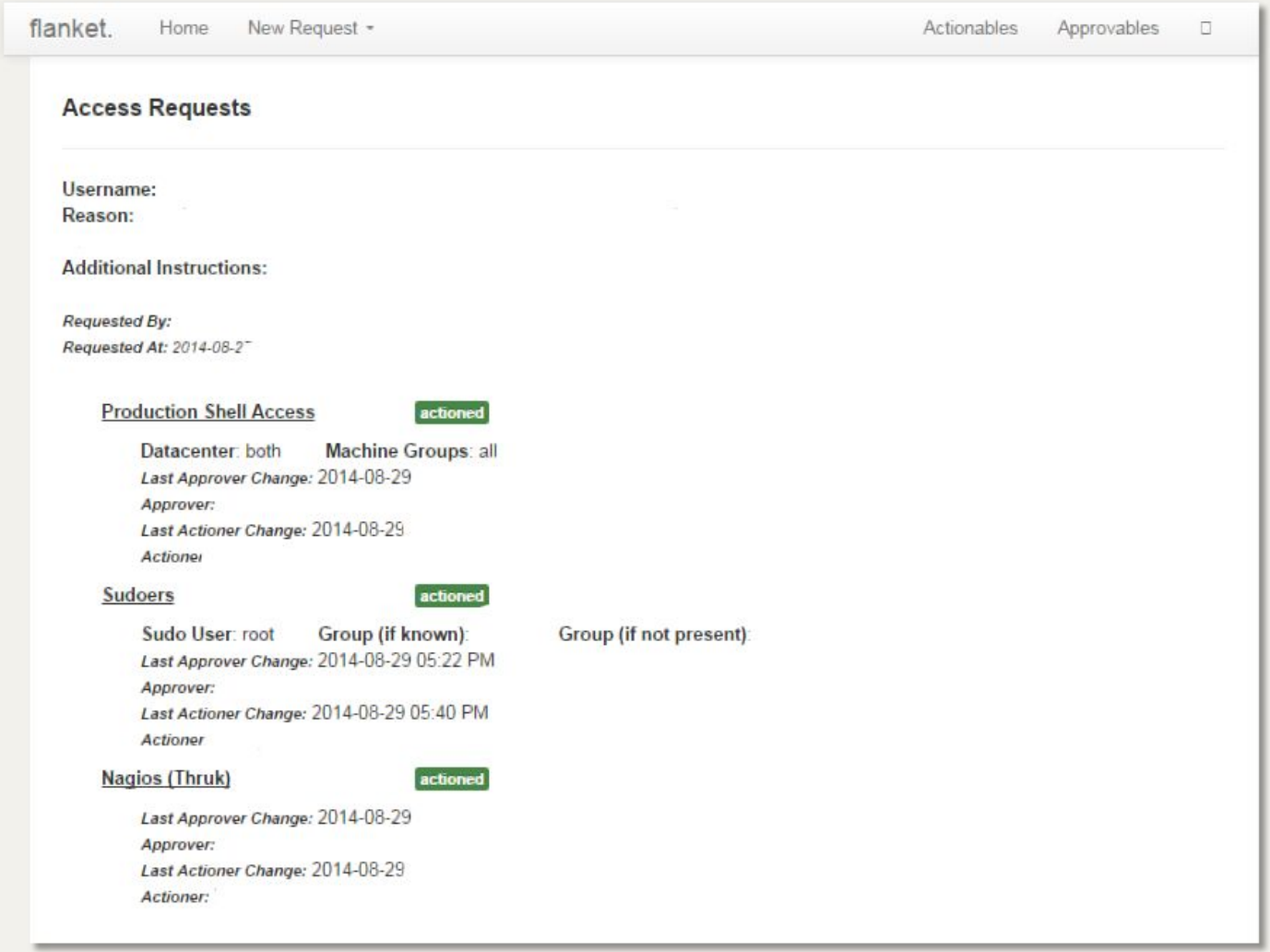
How is access reviewed?






Buy Ave.
Build Rd.

Let's do a little more work...


flanket.
Home
New Request
Actionables
Approvables
Access Requests
Username:
Reason:
Additional Instructions:
Requested By:
Requested At: 2014-08-2
Production Shell Access
actioned
Datacenter: both
Machine Groups: all
Last Approver Change: 2014-08-29
Approver:
Last Actioner Change: 2014-08-29
Actioner
Sudoers
actioned
Sudo User: root
Group (if known):
Group (if not present):
Last Approver Change: 2014-08-29 05:22 PM
Approver:
Last Actioner Change: 2014-08-29 05:40 PM
Actioner
Nagios (Thruk)
actioned
Last Approver Change: 2014-08-29
Approver:
Last Actioner Change: 2014-08-29
Actioner:

flanket

Small improvements...

- Automation
- Report generation



flanket

What we quickly realized...

Teams of users often need the same set of permissions
Teams often share a core set of permissions



flanket

Solution: Templates?







MEROU. Groups Tags Users Permissions Help Search

Users luke_wf@example.com

Group Requests 0 Permission Requests 0

Groups

Name	Role
travis_ci@svc.localhost	np-owner
audit-managers	np-owner
storage-team	owner

Public Keys

Age	Type	Size	Fingerprint	Tags
Yesterday	ssh-rsa	2048	b0:ff:28:37:e9:dc:a3:9c:8f:87:26:80:bf:43:9e:79	

Add Public Key

Permissions

Permission	Argument	From Group	Granted
production.shell	hwrole=magic_pocket	storage-team	40 minutes ago

Access Tokens

Name	Age
MyFirstAccessToken	55 minutes ago

Create access token

Shell

Shell
/bin/false

Change Shell

Passwords

Name	Age
LegacySvc1	55 minutes ago

Create Password

Recent Activity

Date	Actor	Action	Description	Extra

Insert Live Demo Here



Distributed management of groups, permissions, and permission grants

Distributed management

Securely?

Transparent record of activity

Recent Activity

Date	Actor	Action	Description	Extra
2016-07-05 05:45 PM	herb@dropbox.com	grant_permission	Granted permission with argument: blahblahback	Group: group1 Permission: grouper.admin.permissions



"Who gave a sales engineer access to prod?!"



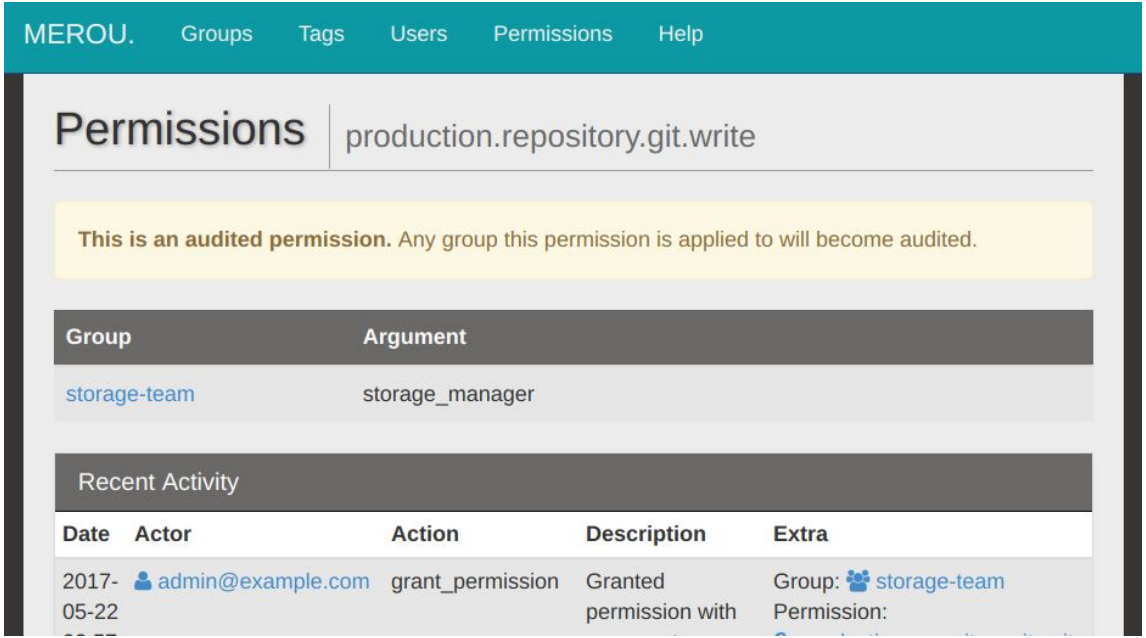
"Why does that sales engineer *still* have access to prod?!"



Distributed **auditing**

Distributed auditing

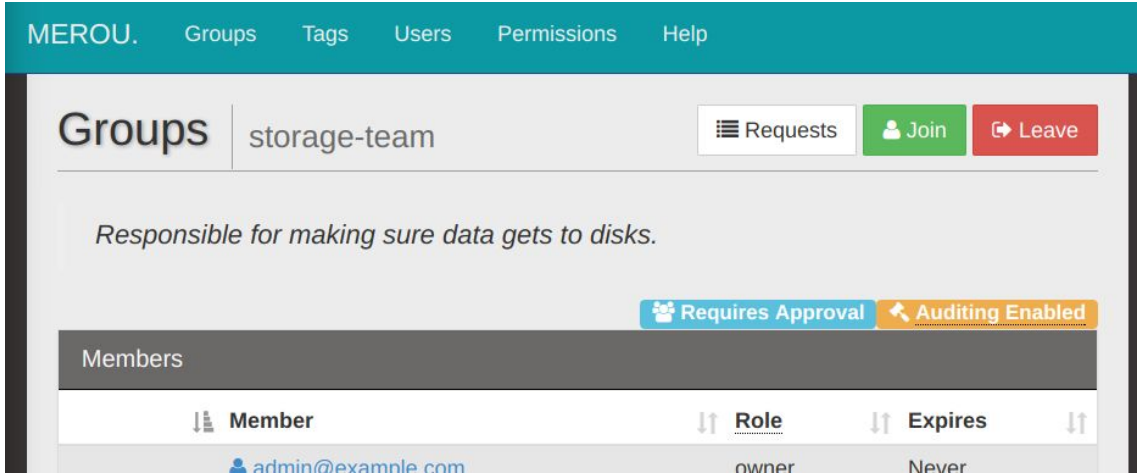
Permissions can be marked as *audited*.



Distributed auditing

Permissions can be marked as *audited*.

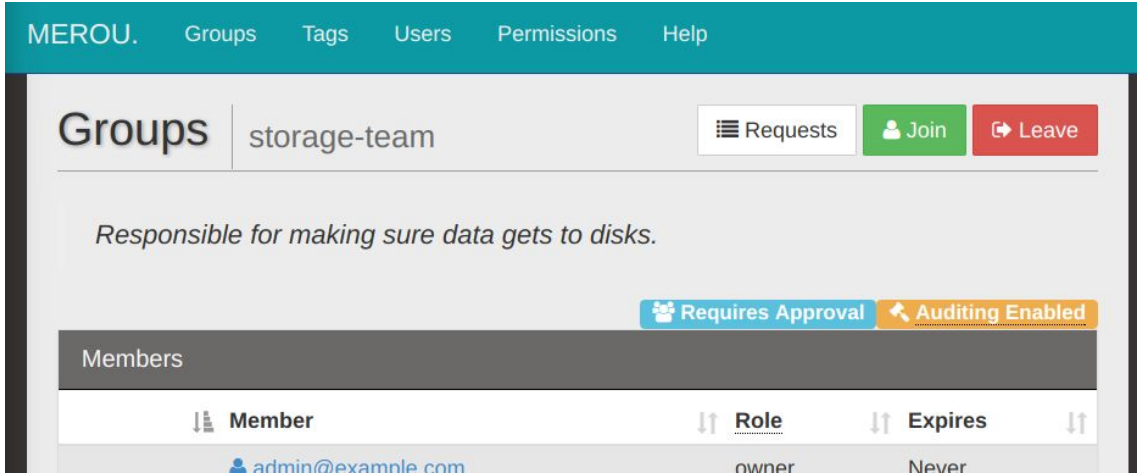
Groups that have been granted audited permissions become **audited groups**.



Distributed auditing

Permissions can be marked as *audited*.

Groups that have been granted audited permissions become **audited groups**.

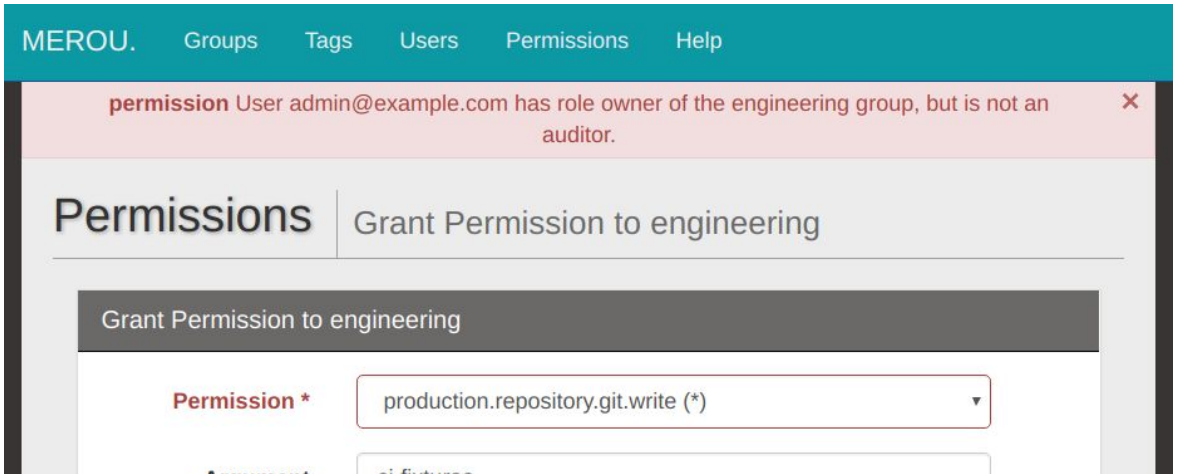


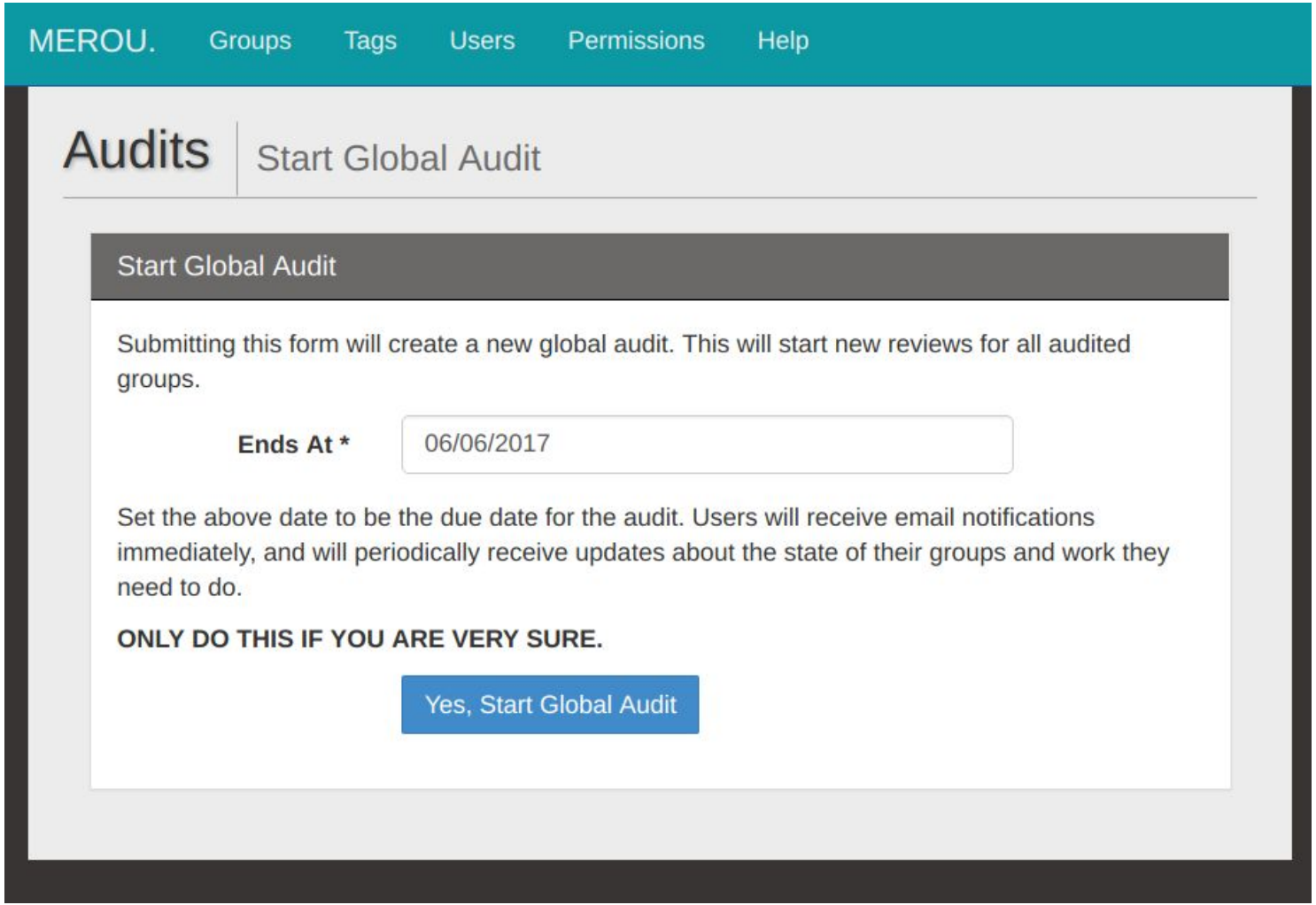
Distributed auditing

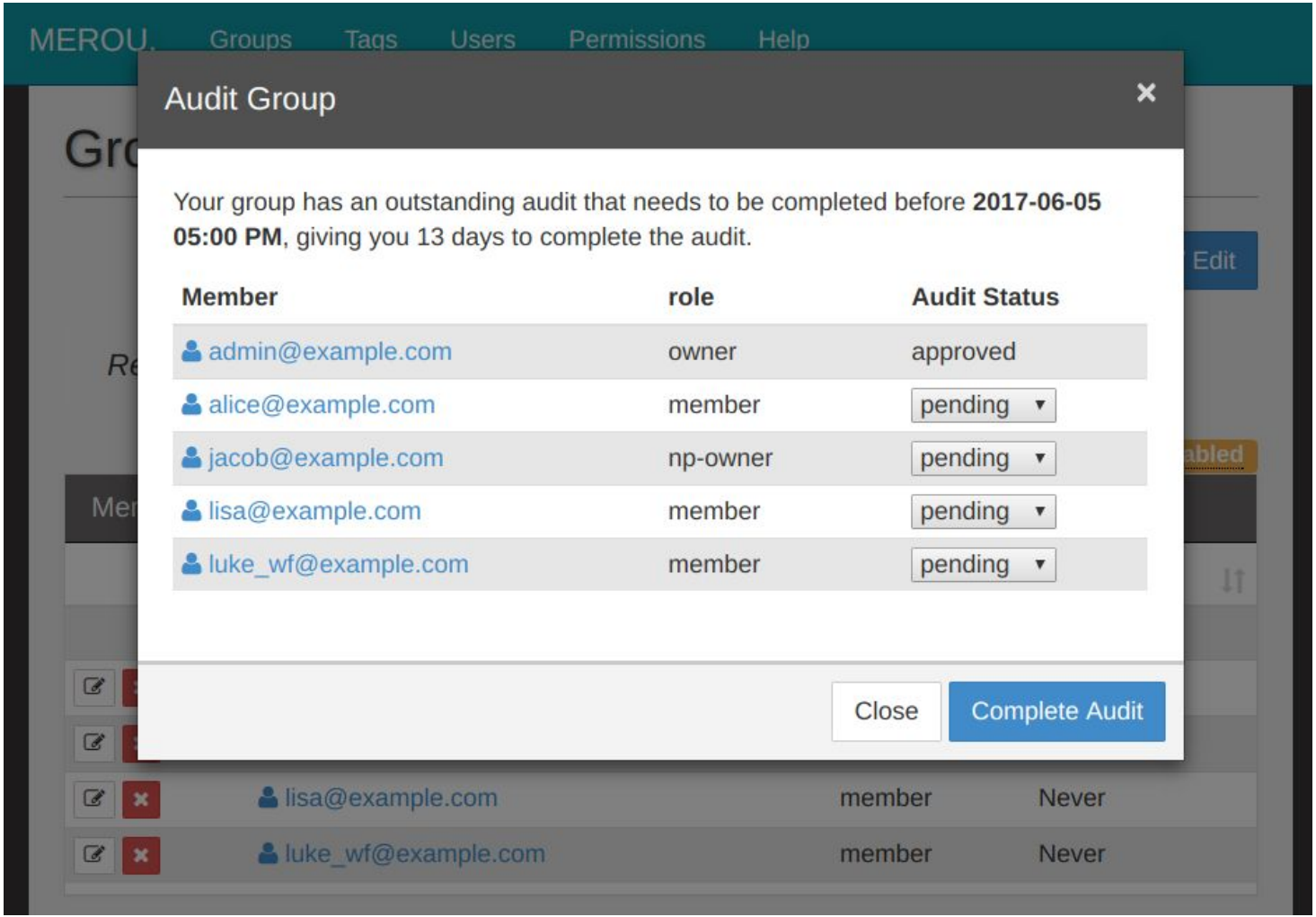
Permissions can be marked as *audited*.

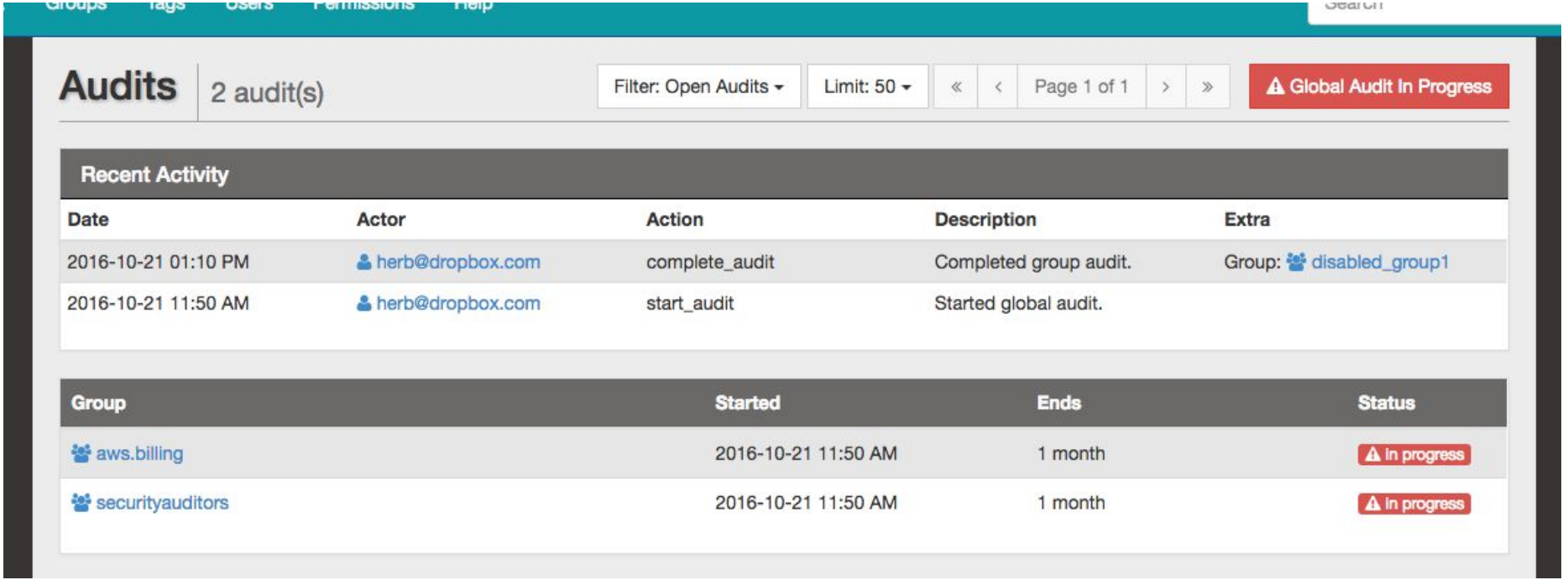
Groups that have been granted audited permissions become **audited groups**.

Owners of audited groups first undergo **audit training**.




MEROU.
Groups
Tags
Users
Permissions
Help
Audits
Start Global Audit
Start Global Audit
Submitting this form will create a new global audit. This will start new reviews for all audited groups.
Ends At *
06/06/2017
Set the above date to be the due date for the audit. Users will receive email notifications immediately, and will periodically receive updates about the state of their groups and work they need to do.
ONLY DO THIS IF YOU ARE VERY SURE.
Yes, Start Global Audit


MEROU.
Groups
Tags
Users
Permissions
Help
Audit Group
Your group has an outstanding audit that needs to be completed before **2017-06-05 05:00 PM**, giving you 13 days to complete the audit.
Member
role
Audit Status
admin@example.com
owner
approved
alice@example.com
member
pending
jacob@example.com
np-owner
pending
lisa@example.com
member
pending
luke_wf@example.com
member
pending
Close
Complete Audit
lisa@example.com
member
Never
luke_wf@example.com
member
Never


Groups
Tags
Users
Permissions
Help
Search
Audits
2 audit(s)
Filter: Open Audits
Limit: 50
Page 1 of 1
Global Audit In Progress
Recent Activity
Date
Actor
Action
Description
Extra
2016-10-21 01:10 PM
herb@dropbox.com
complete_audit
Completed group audit.
Group: disabled_group1
2016-10-21 11:50 AM
herb@dropbox.com
start_audit
Started global audit.
Group
Started
Ends
Status
aws.billing
2016-10-21 11:50 AM
1 month
In progress
securityauditors
2016-10-21 11:50 AM
1 month
In progress

(content cut for time)



Takeaways

Merou!

Transparency and democracy work
... when paired with process and tools.

Let other people do your work for you
... but make their jobs' easy.



Thanks for listening!



Epinephelus malabaricus, a.k.a. the Malabar Grouper
(Image: jon hanson from london, UK; CC-BY-SA 2.0)

github.com/dropbox/merou

luke@dropbox.com

