Internet2 Techex 2018

Latest Grouper Recipes

Chris Hyzer, University of Pennsylvania
Michael Gettes, Florida
Chad Redman, UNC-Chapel Hill
Chris Sutherin, UMBC
Bert Bee-Lindgren, Georgia Tech
John Gasper, Unicon
Carl Waldbieser, Lafayette College
James Babb, Internet2

Agenda

- Lightning talks
- Cool things
- Done recently
- In grouper
- Extra points for integrating with other Internet2 products
- More information of each documented in Community Contributions in wiki

Internet2 Techex 2018

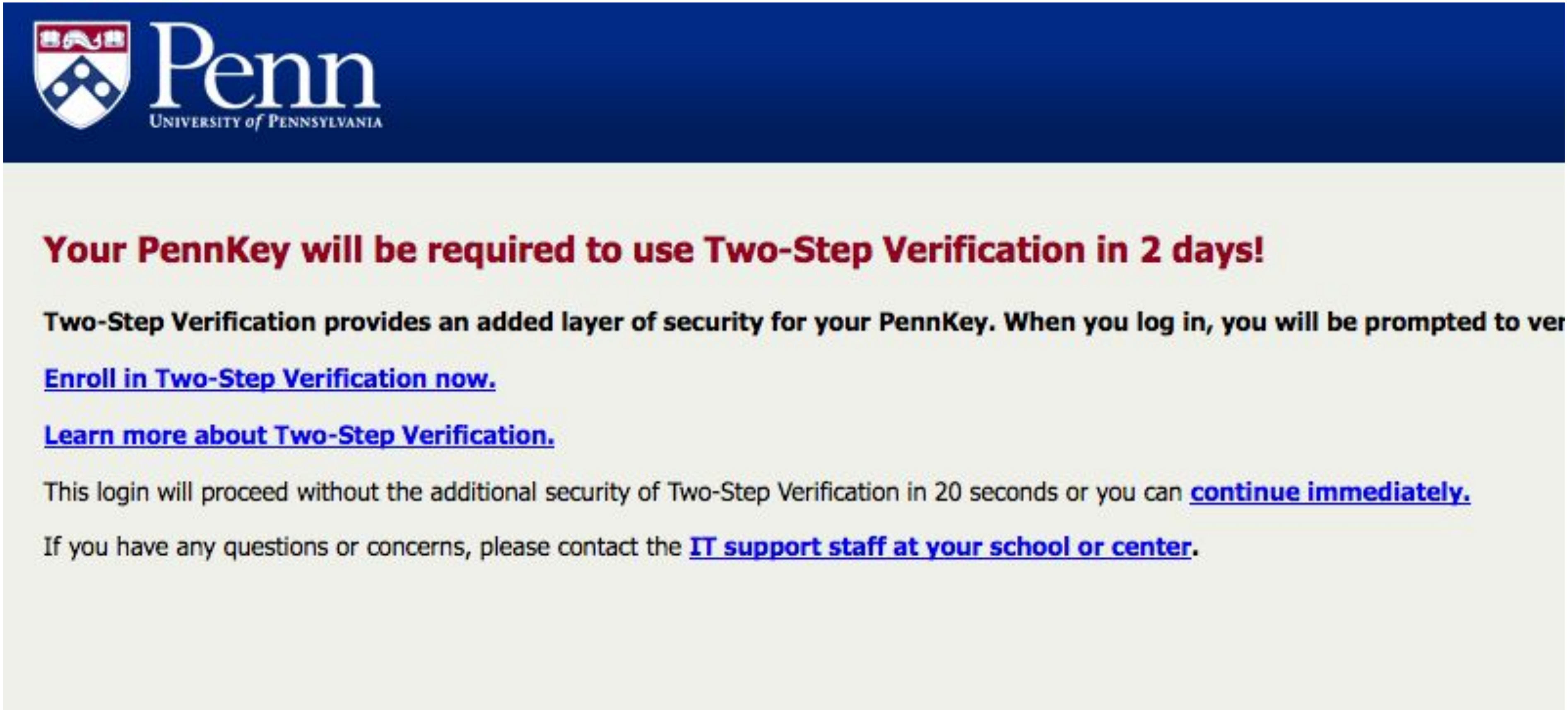
Chris Hyzer

Latest Grouper Recipes

Two-step countdown intercept page

- When a population is soon to be required to use two-step MFA
- Give them a warning on login (9 days left, 8 days left, etc) until they enroll
- For more information see the community contribution site

Two-step countdown intercept page (continued)



Your PennKey will be required to use Two-Step Verification in 2 days!

Two-Step Verification provides an added layer of security for your PennKey. When you log in, you will be prompted to ver

Enroll in Two-Step Verification now.

Learn more about Two-Step Verification.

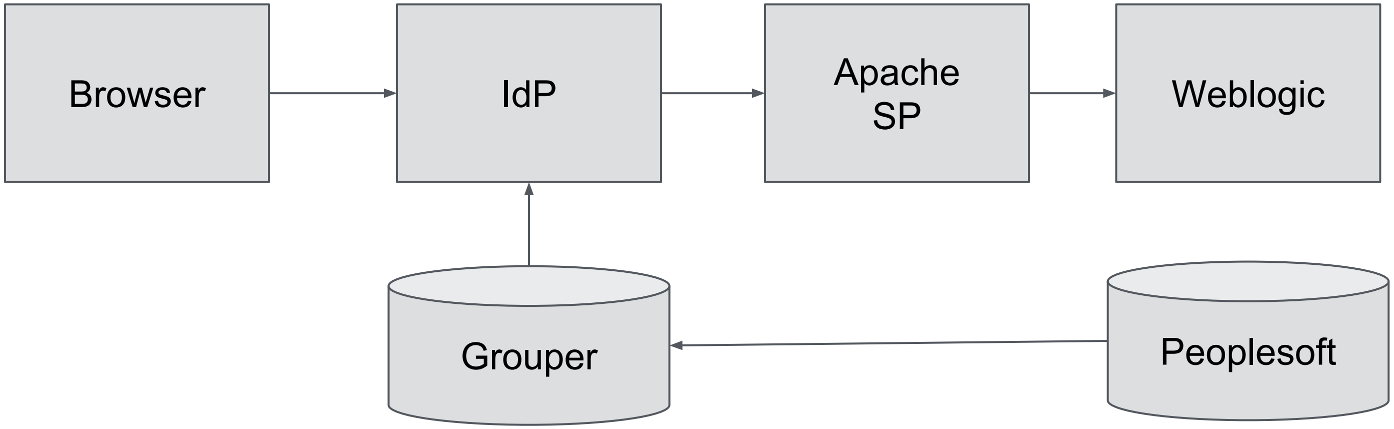
This login will proceed without the additional security of Two-Step Verification in 20 seconds or you can continue immediately.

If you have any questions or concerns, please contact the IT support staff at your school or center.

Two-step countdown intercept page

- Attribute on a group, with value of a required date, e.g. 2018/10/31
- Some views which the loader uses to make groups based on if enrolled, make 9 groups
  - 9 day warning
  - 8 day warning (etc)
  - 0th day puts them in a group to be required
- Shibboleth magic to turn those groups into warning screen

Coarse-grained authorization



- We’ve been doing a lot of coarse-grained authorization
- We only allow traffic through the IdP or if local apache, to the SP based on group
- Contrib page

Coarse-grained authorization

- Get a view from application
- Get database link to grouper database
  - To read that view
- Make a course-grained group
- Intersect with active employee group
- Reflect that as SAML entitlement
- Restrict that in Apache:

```
Require shib-attr entitlement
urn:mace:upenn.edu:penn:app:ps:psProd
```

Feed door access from ccure to Grouper

- Get a feed of ccure data (via email?!#)
- Make an “otherJob” in java which get the mail and updates a SQL table
  - Use the grouper client ORM
- Use the loader to load groups
- Have an overall group, and minus activeEmployee
- Resulting list is door access to remove
- Community contrib

Add attributes on objects based on name

- Request from Jeff Williams (UNCG) to add DNP to any “ref” or “etc” groups
- This is an example that might help many other areas (e.g. DNP include/exclude)
- Grouper rule
- On stem (or group) create
- If name pattern matches
- Add attributes (DNP ldap and ad)
- Link to wiki for stem rules
- Link to wiki for group rules

Internet2 Techex 2018

Michael Gettes

Latest Grouper Recipes

Grouper Visualization - GRAPHS!

- Grouper UI - it is what it is.
- Developing access policies can get complicated - as you combine groups, composites are used to join and filter populations. Many groups, inter-related.
    - Did I get my group service/access policy right?
    - How do I help the App Admin understand?
    - If only I can show how grouper objects relate?
    - How can I visualize complexities in Grouper?

Graphing Grouper

Recipe for proof of concept:

- 1lb of dockerized grouper (doper?)
- 3lbs of learning groovy
- 2lbs of graphviz.org
- 5g of Carey Black’s help!

Run shell script to feed docker-gsh to run a sizeable groovy script to generate output for graphviz which generates SVG to present a graph-view of Grouper

Sample Graphs

https://spaces.at.internet2.edu/x/FoInC

Grouper Community Contributions - University of Florida

Now discussing how to move from proof of concept to incorporating into Grouper

Graphs are dynamically generated.

Start at a group/folder or a subject.

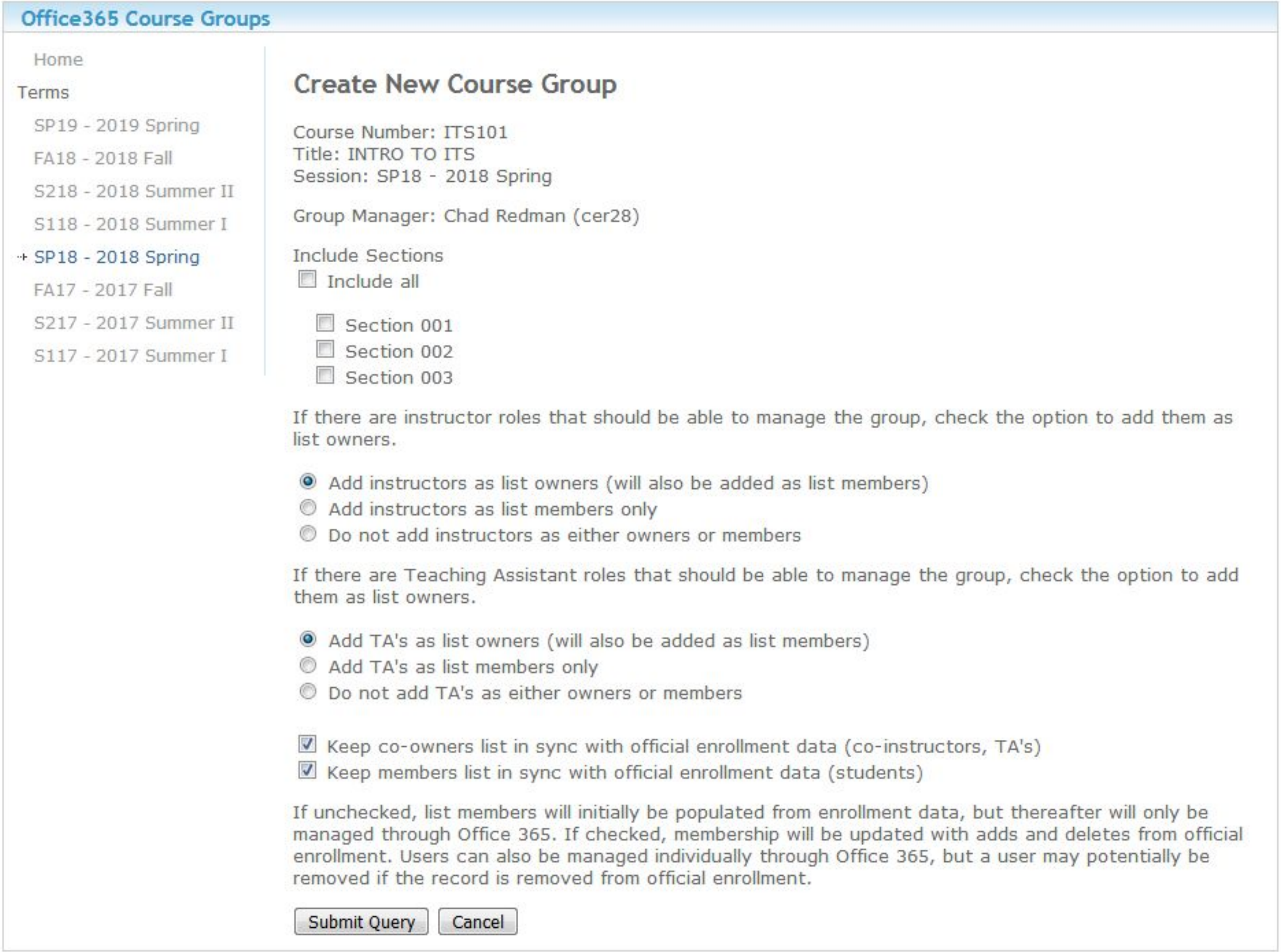
Graphs "dependencies" from start point.

Internet2 Techex 2018

Chad Redman

Latest Grouper Recipes

Course Groups for Office 365



Office365 Course Groups

Create New Course Group

Course Number: ITS101
Title: INTRO TO ITS
Session: SP18 - 2018 Spring

Group Manager: Chad Redman (cer28)

Include Sections
□ Include all

□ Section 001
□ Section 002
□ Section 003

If there are instructor roles that should be able to manage the group, check the option to add them as list owners.

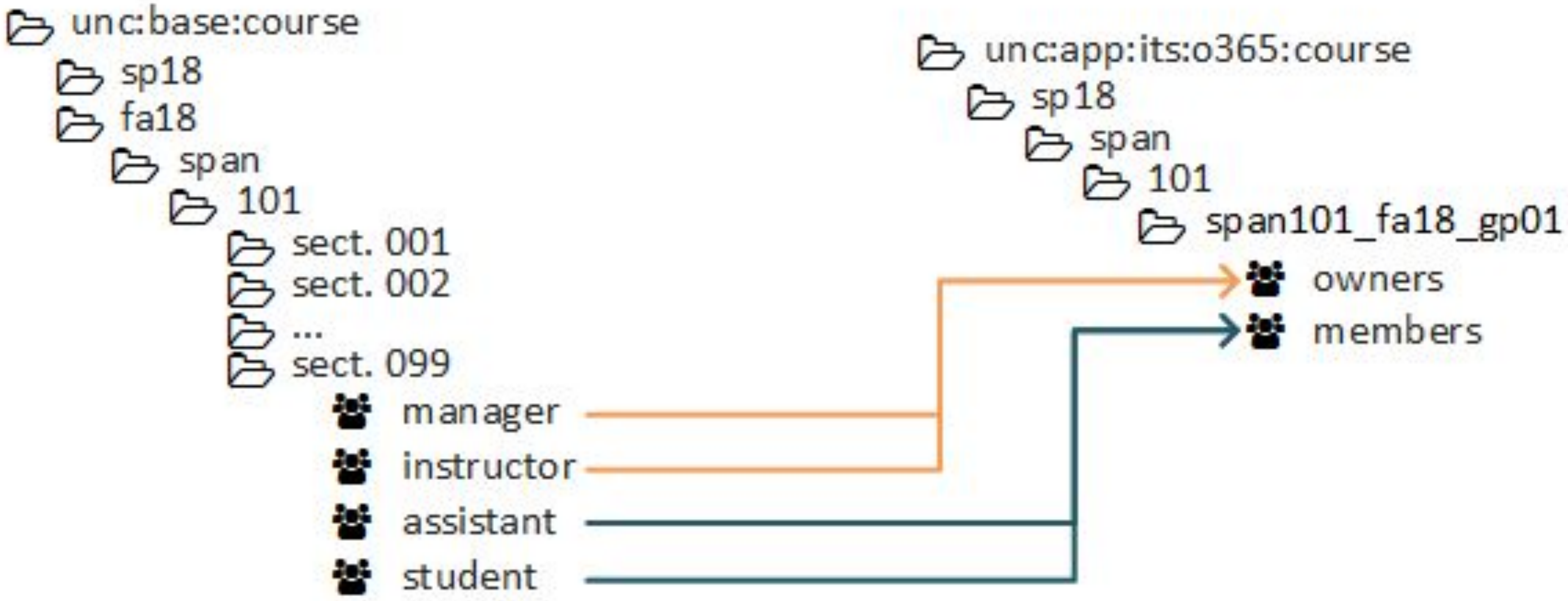
● Add instructors as list owners (will also be added as list members)
○ Add instructors as list members only
○ Do not add instructors as either owners or members

If there are Teaching Assistant roles that should be able to manage the group, check the option to add them as list owners.

● Add TA's as list owners (will also be added as list members)
○ Add TA's as list members only
○ Do not add TA's as either owners or members

☑ Keep co-owners list in sync with official enrollment data (co-instructors, TA's)
☑ Keep members list in sync with official enrollment data (students)

If unchecked, list members will initially be populated from enrollment data, but thereafter will only be managed through Office 365. If checked, membership will be updated with adds and deletes from official enrollment. Users can also be managed individually through Office 365, but a user may potentially be removed if the record is removed from official enrollment.



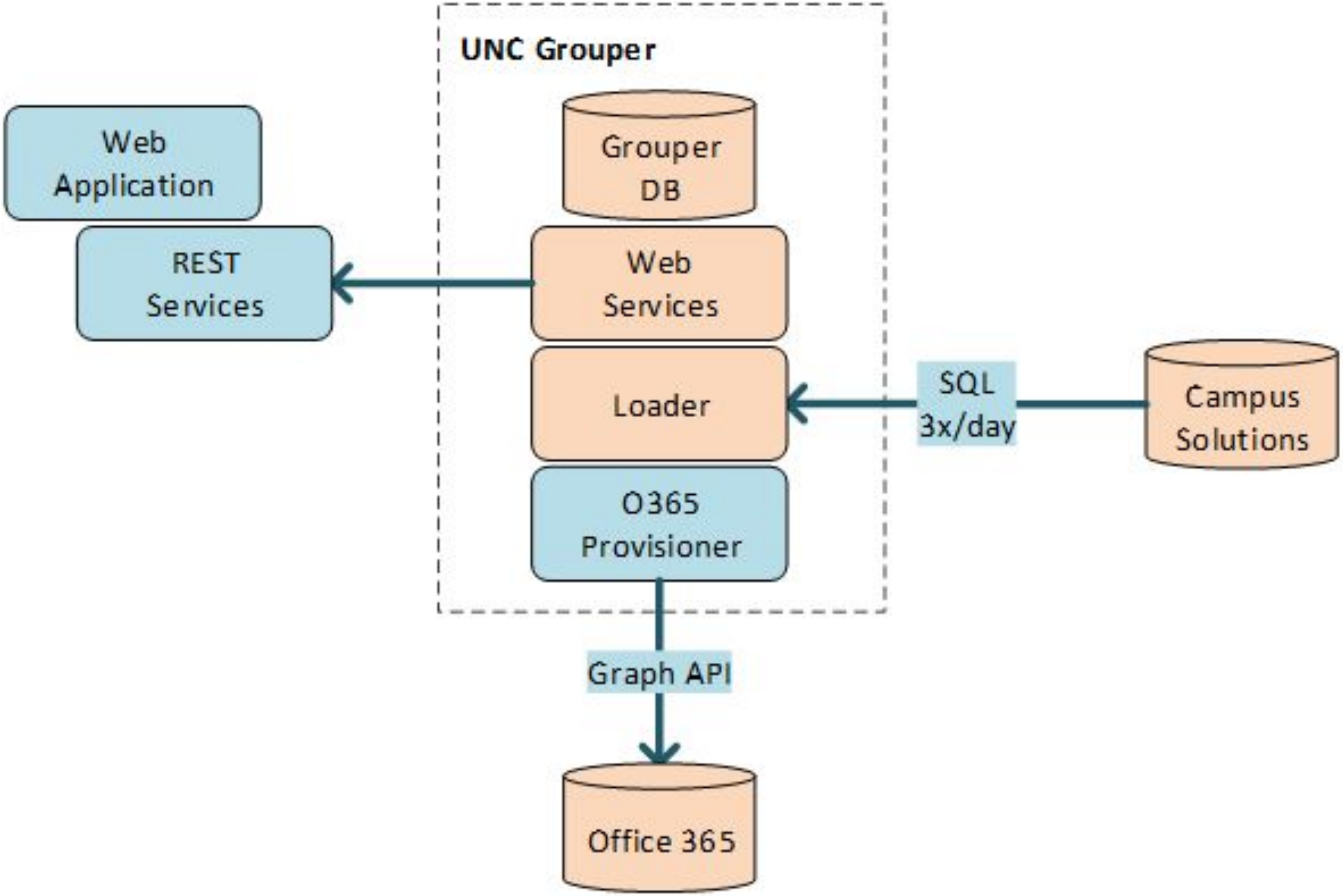
Basis Groups

- unc:base:course
  - sp18
  - fa18
    - span
      - 101
        - sect. 001
        - sect. 002
        - …
        - sect. 099
          - manager
          - instructor
          - assistant
          - student

App Groups

- unc:app:its:o365:course
  - sp18
    - span
      - 101
        - span101_fa18_gp01
          - owners
          - members

Architecture



Architecture Summary

- 4 Loader jobs (SQL groups list) sync 3x/day
  - 160,000 groups, 380,000 memberships (88% are students)
  - 10 minutes per job (2.3.0), 55 minutes per job (2.4.0)
- WS marginally works as a persistence back end
  - WS is not SQL!
  - Need workarounds and multiple calls (e.g., no joins)
  - Using ehcache to boost performance
- Changelog consumer to sync with Office 365
  - Based on Unicon's Azure AD connector (office365-and-azure-ad-grouper-provisioner)
  - Modified to support separate members and owner groups
  - Added more config options (more attributes, EL to construct O365 name)
- Details at Community Contribution site

Open Source Rules!

- All bugs are shallow
  - Using WS in creative ways uncovered a few bugs (two where clauses, attribute consumer required debug log level)
- A mutual benefit
  - We can trace the code to understand behavior
  - We can modify the source to fit our needs
  - We can submit patches to Grouper, everyone benefits!
  - Enhancements too: WS now accepts application/json content type
- Much gratitude to Unicon for Office 365 Provisioner
  - Gave us 90% of what we needed, saving many hours

Internet2 Techex 2018

Chris Sutherin

Latest Grouper Recipes

Google provisioner

The Problem

UMBC has the desire to replicate certain portal groups into Google as an automated process. This will allow us to leverage Google capabilities. Initially we are using it for email groups as a proof of concept.

Potential future use would include creating shared folders for classes along with the associated email group. These could be built as the section and class level.

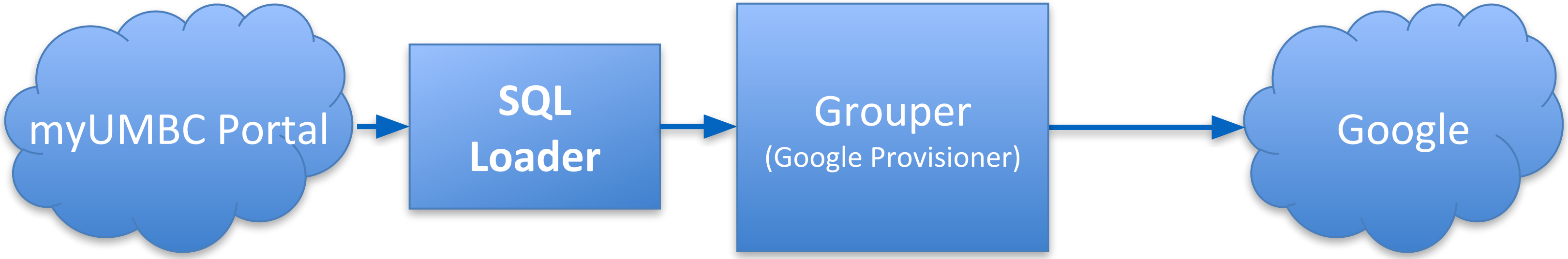
Solution

The solution to our problem is the Google provisioner. We now provision portal groups into Google. The provisioner supports multiple provisioner instances/configurations fine-grain control over which groups are provisioned and the ability to configure Google's "advanced" group settings.

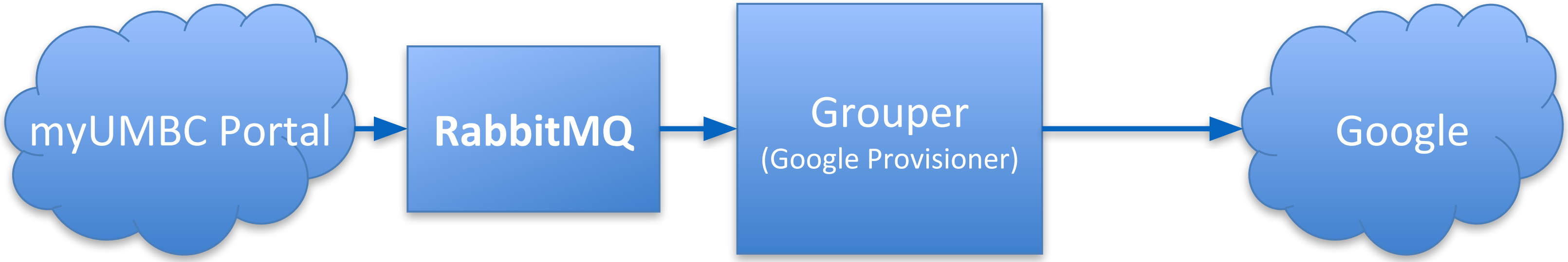
Remaining work will include modifying our portal to allow group owners the option to provision to Google.

Workflow

Today



Soon



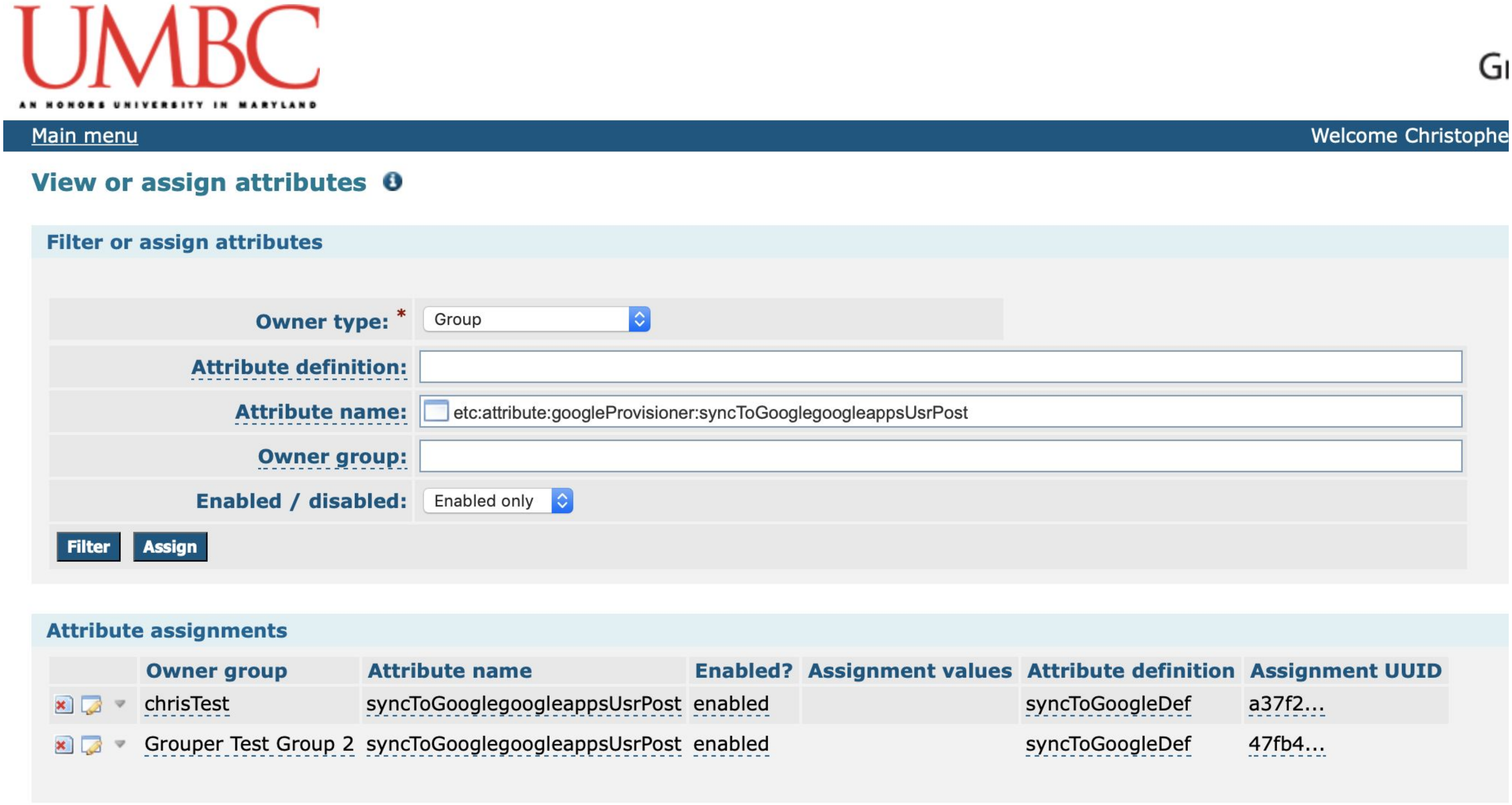
Grouper loader properties example

```
# Google Processing Controls

changeLog.consumer.googleappsUsrPost.groupIdentifierExpression=${groupPath.replaceAll(".*:","").replaceAll("([A-Z]+)", "-$1")}-group

changeLog.consumer.googleappsUsrPost.whoCanManage=admin

# Google Group Settings
changeLog.consumer.googleappsUsrPost.whoCanPostMessage=ALL_MANAGERS_CAN_POST
```



View or assign attributes

Filter or assign attributes

Owner type: *	Group
Attribute definition:	
Attribute name:	etc:attribute:googleProvisioner:syncToGooglegoogleappsUsrPost
Owner group:	
Enabled / disabled:	Enabled only

Attribute assignments

	Owner group	Attribute name	Enabled?	Assignment values	Attribute definition	Assignment UUID
	chrisTest	syncToGooglegoogleappsUsrPost	enabled		syncToGoogleDef	a37f2...
	Grouper Test Group 2	syncToGooglegoogleappsUsrPost	enabled		syncToGoogleDef	47fb4...

Internet2 Techex 2018

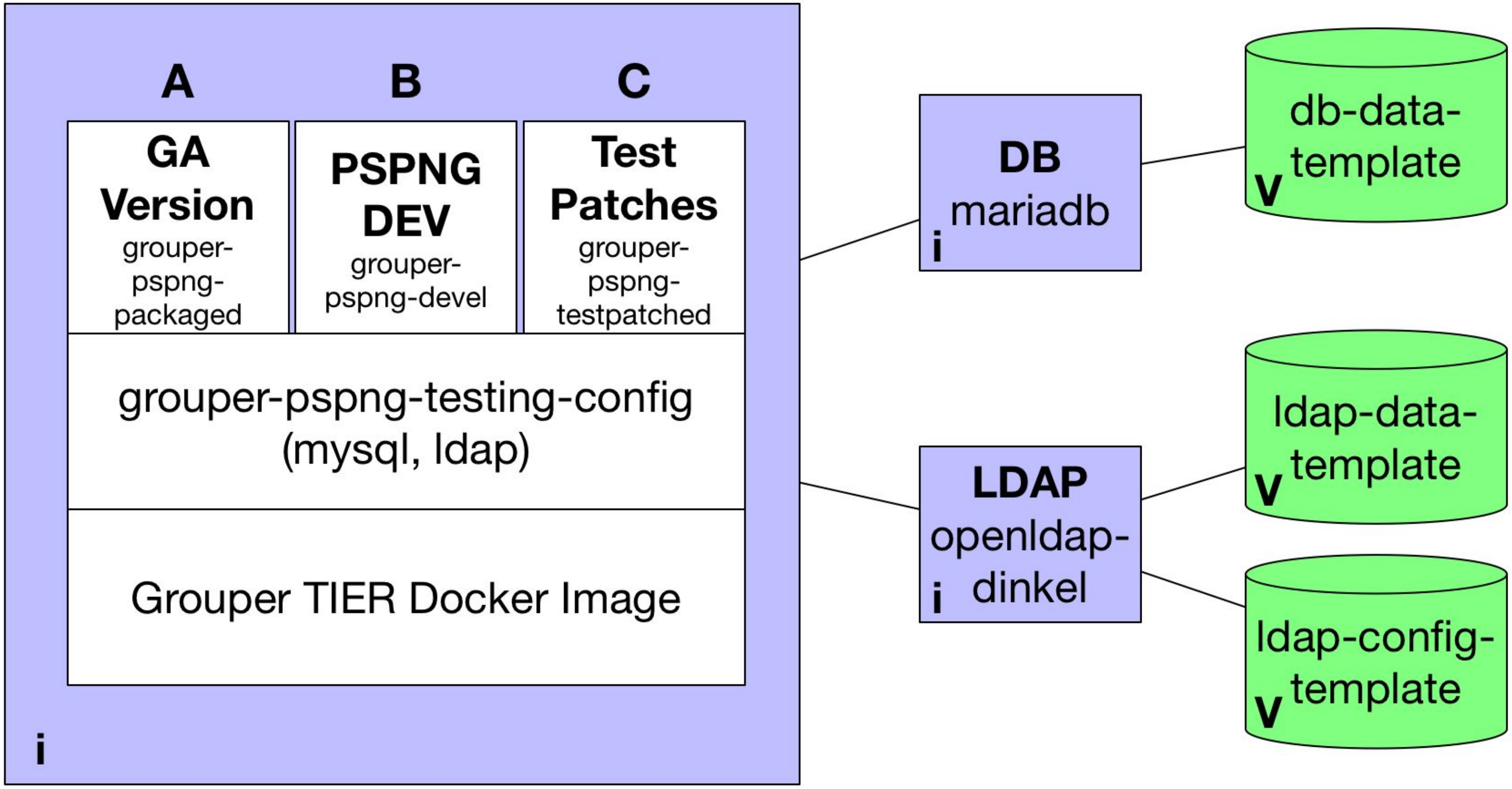
Bert Bee-Lindgren

Latest Grouper Recipes

PSPNG dockerized testing

- Why
  - Test-driven development
  - Catch regressions & patching mistakes
- How
  - Spin up Grouper Daemon, DB, LDAP
  - Control
  - Destroy
  - Repeat
- Where:
  - grouper-pspng/pspng-docker-tests

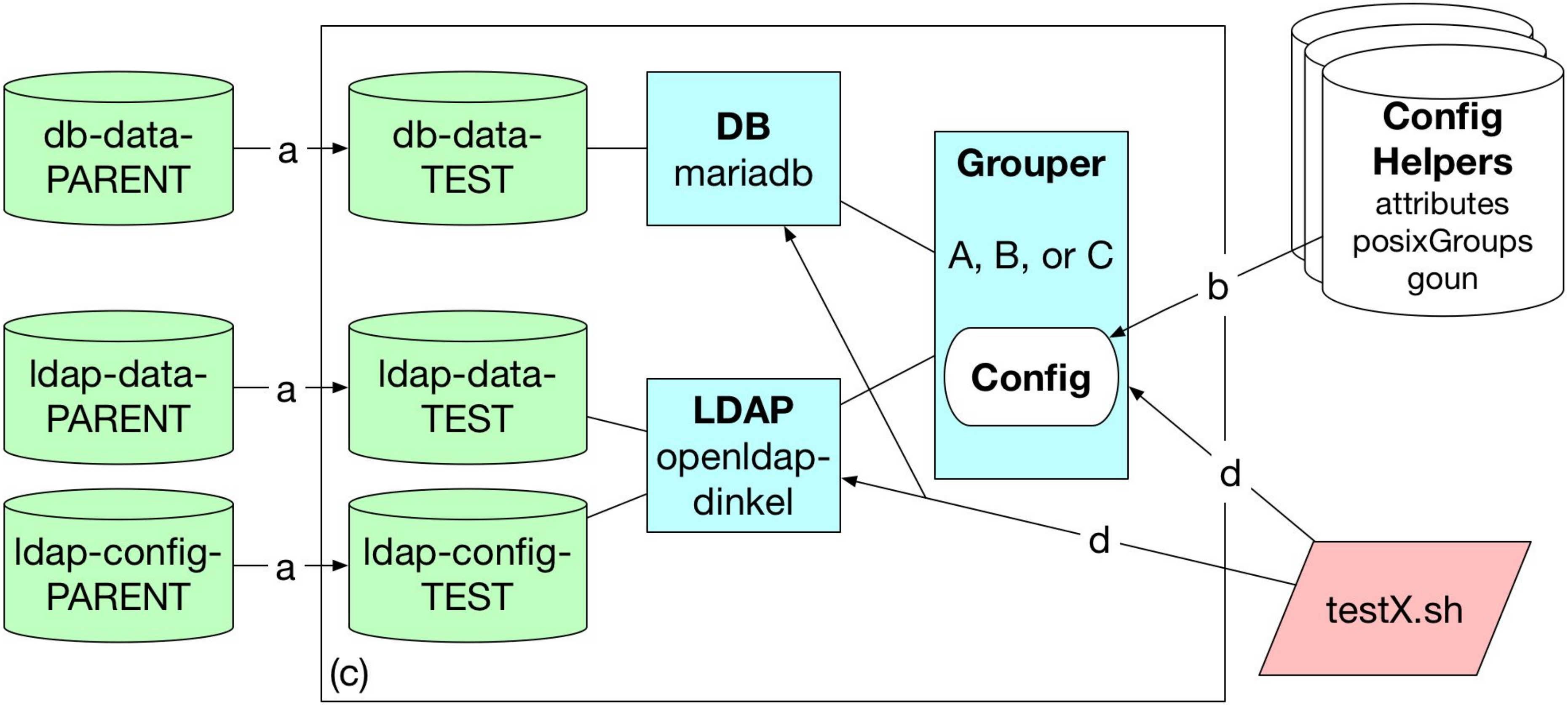
1 Prepare



1
build-images

2
build-data-templates

2 Test - testSomething.sh



a: clone parent/template vols

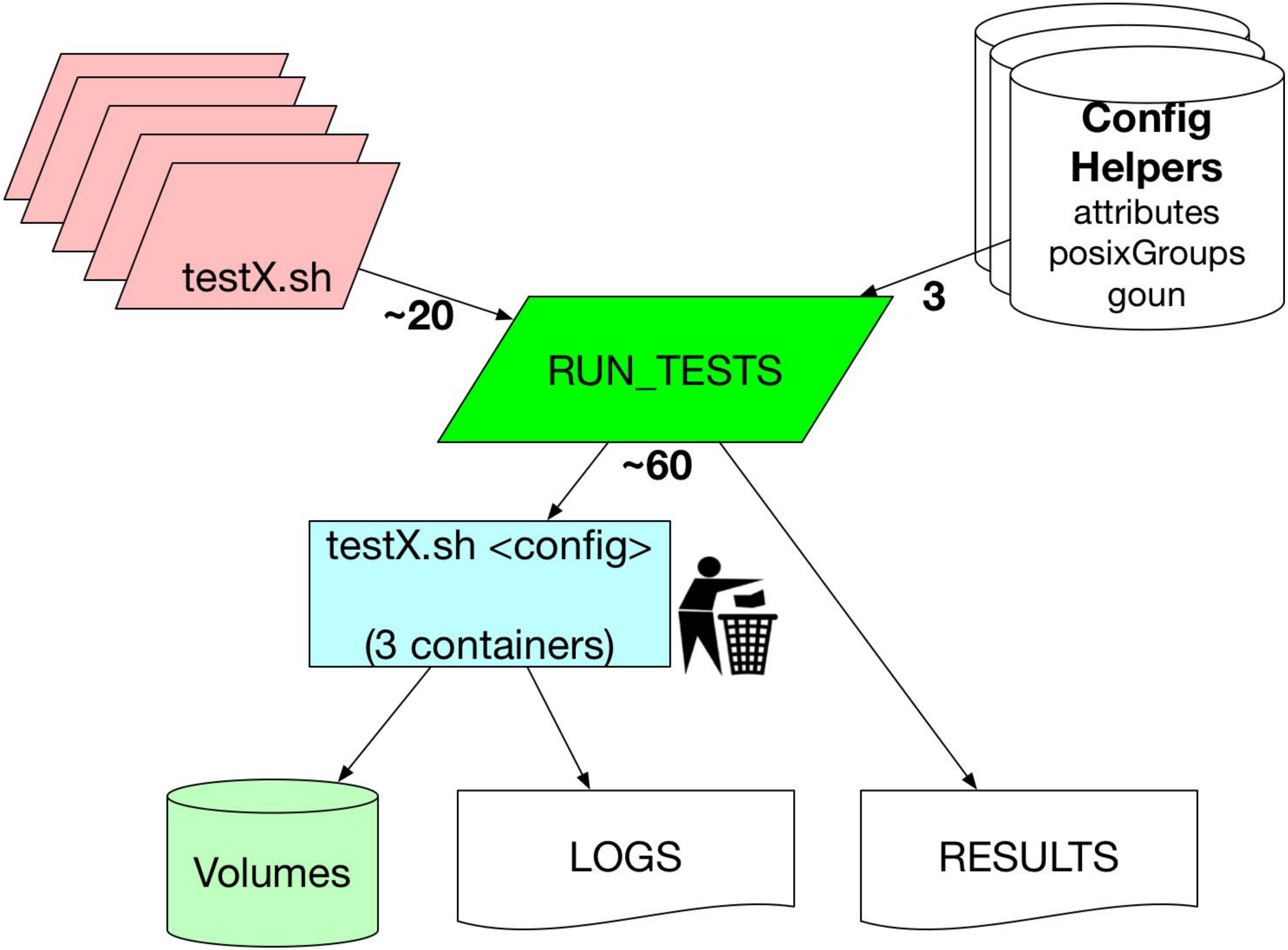
b: set up config files

c: docker-compose up

d: DO TEST - gsh, ldap & db

e: cleanup if successful

3 Harness - RUN_TESTS



Internet2 Techex 2018

John Gasper

Latest Grouper Recipes

Getting started with the TIER Docker Image

- Video tutorial for deploying the TIER Grouper Image with Docker Swarm
- Tutorial Project: https://github.com/Unicon/tier-grouper-deployment
- Video Series: https://www.youtube.com/watch?v=750J5UBTctw

Jenkins Pipeline to update Swarm

- Commits to SCM fires Jenkins Pipeline
- Custom images are built and published to repo
- Docker Swarm is told to update Grouper services (UI, WS, Loader/Daemon) in parallel.
- https://www.unicon.net/about/blogs/continuous-delivery-grouper-using-jenkins-and-docker

Internet2 Techex 2018

Carl Waldbieser

Latest Grouper Recipes

Provisioning via cron and messaging example

- At Lafayette we have a rich IAM provisioning pipeline based on message routing via RabbitMQ.
- We have provisioners capable of targeting REST & web based APIs, shells via SSH, LDAP, extensible.
- Our latest provisioning challenge was to an extremely sophisticated target ...

Three Words

High-Tech

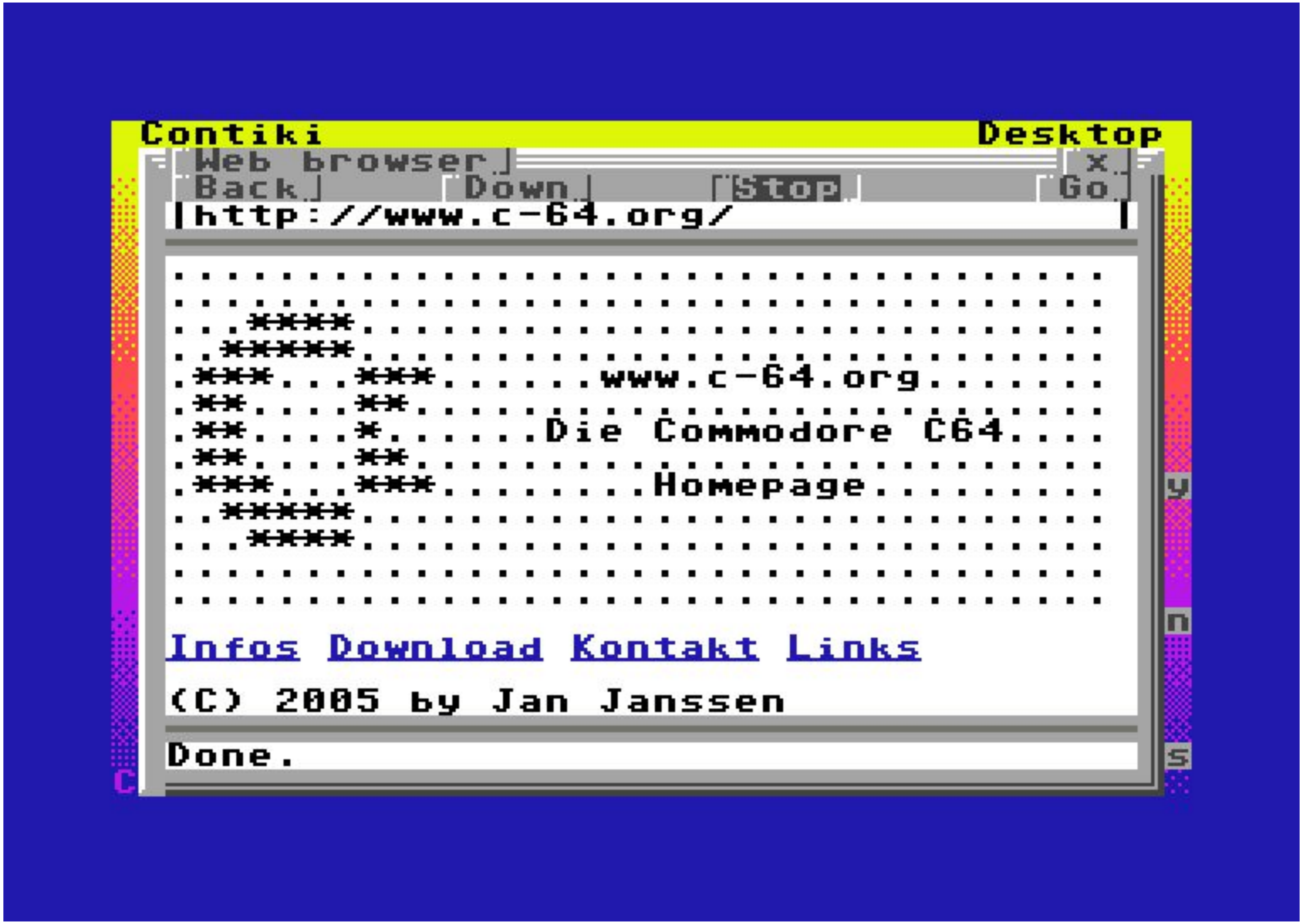
We were working with an integration partner for our PaaS scheduling system. After explaining the capabilities of our provisioning infrastructure and asking what kind of API they support, they responded with, flat file transfer over SFTP. And not just any SFTP ...

Umm, what is “key-based”?

Username: Administrator

Password: ●●●●●●●●●

Old School Meets New School



http://www.c-64.org/

```
...................................
...................................
...*****............................
..******............................
.***...***......www.c-64.org.......
.**....**..........................
.**....*......Die Commodore C64....
.**....**..........................
.***...***........Homepage.........
..******............................
...*****............................
...................................
...................................
```

Infos Download Kontakt Links

(C) 2005 by Jan Janssen

Done.

Cron!

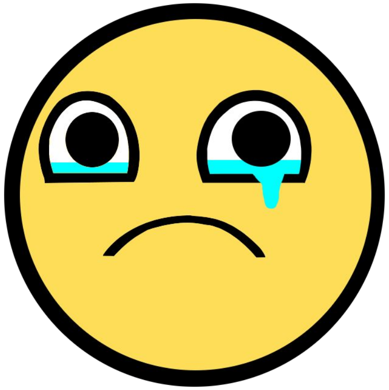
Internet2 Techex 2018

James Babb

Latest Grouper Recipes

Grace Period Groups

- Box Eligibility:
  - All Current Employees, All Currently Enrolled Students, etc. Login stopped at IdP if not eligible.
- Problem:
  - I stopped working at UW. How do I get my files off Box?



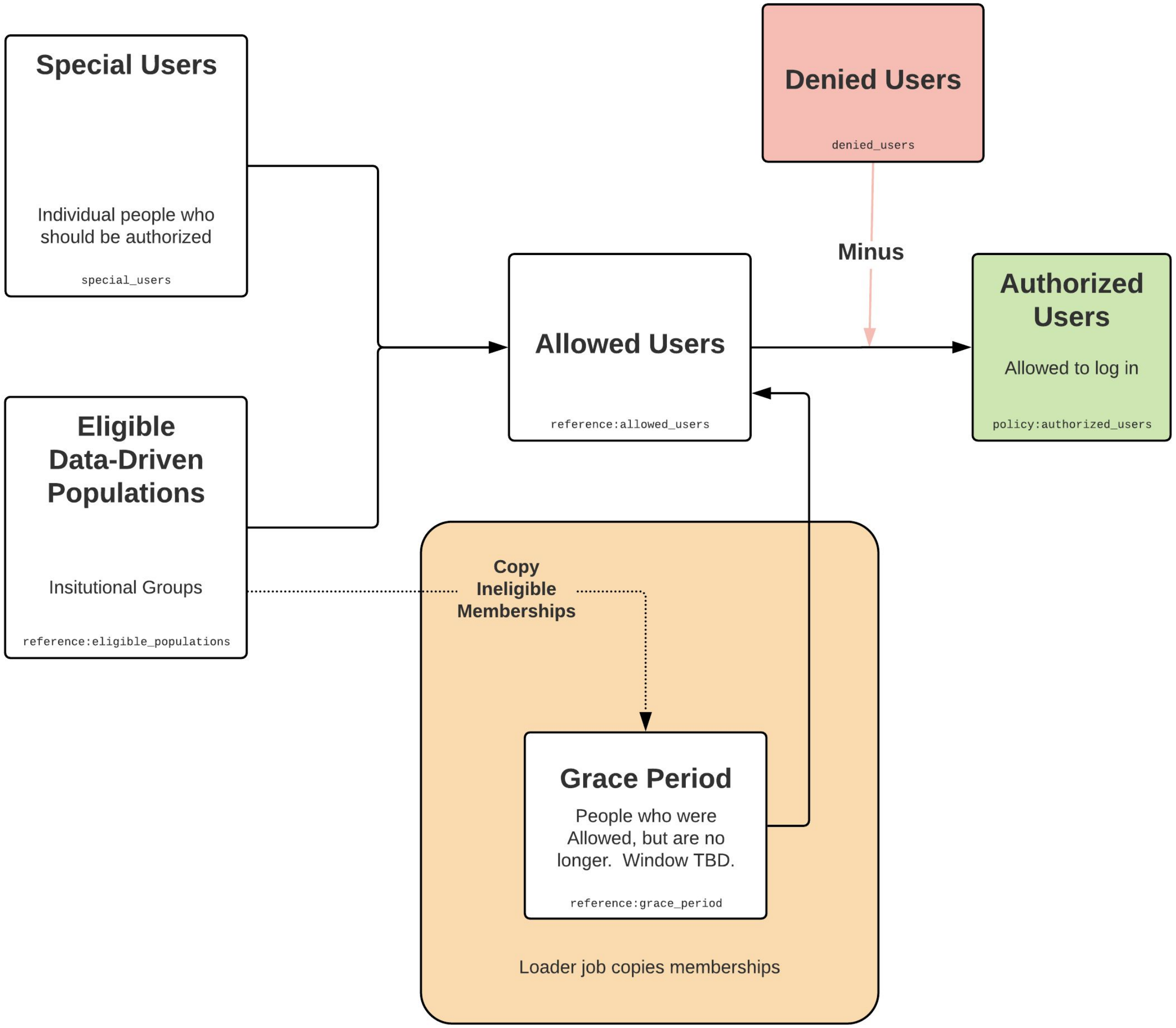
Grace Period Groups

- Could build in to basis groups
  - Make a “Former Employees” for a time period (a year?) after last employment date

- Problem 2:
  - Varying definitions of grace periods
  - Box -> 90 Days
  - Qualtrics -> 30 Days
  - Office 365 -> 2 Years

Grace Period Groups

Version 1 (Box)



Special Users

Individual people who should be authorized

special_users

Eligible Data-Driven Populations

Insitutional Groups

reference:eligible_populations

Allowed Users

reference:allowed_users

Denied Users

denied_users

Minus

Authorized Users

Allowed to log in

policy:authorized_users

Copy Ineligible Memberships

Grace Period

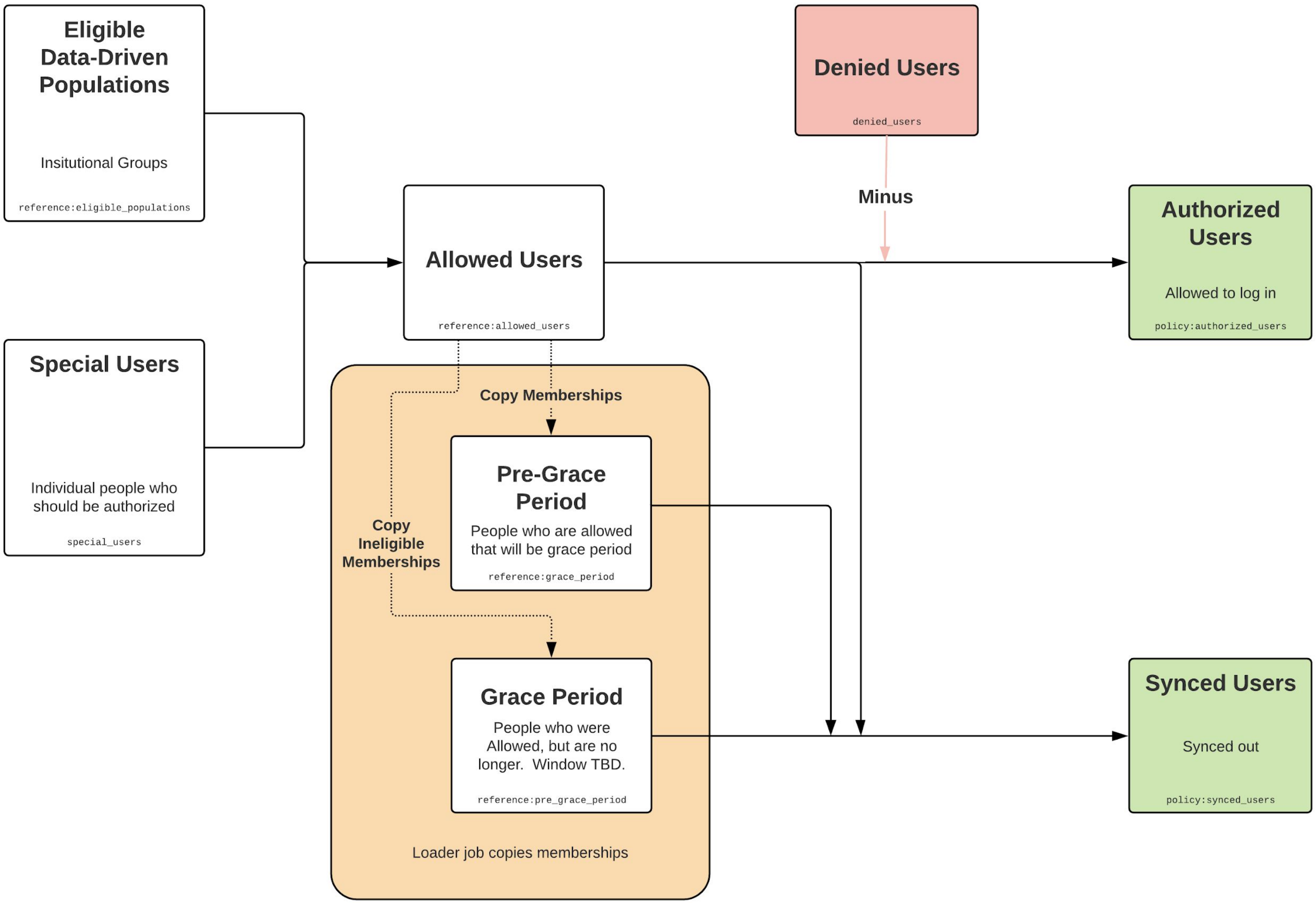
People who were Allowed, but are no longer. Window TBD.

reference:grace_period

Loader job copies memberships

Grace Period Groups

Version 2 (Cisco WebEx)



Eligible Data-Driven Populations

Insitutional Groups

reference:eligible_populations

Special Users

Individual people who should be authorized

special_users

Allowed Users

reference:allowed_users

Denied Users

denied_users

Minus

Authorized Users

Allowed to log in

policy:authorized_users

Copy Memberships

Copy Ineligible Memberships

Pre-Grace Period

People who are allowed that will be grace period

reference:grace_period

Grace Period

People who were Allowed, but are no longer. Window TBD.

reference:pre_grace_period

Loader job copies memberships

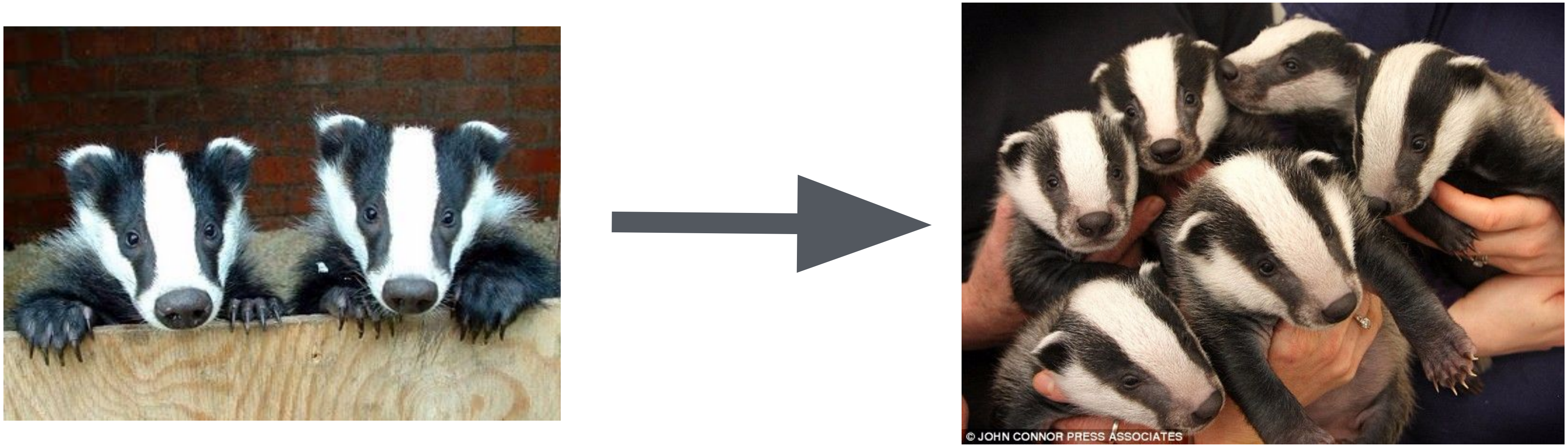
Synced Users

Synced out

policy:synced_users

Grace Period Groups - Next Steps

- Make this scalable using Grouper attributes
- Single Loader Job



© JOHN CONNOR PRESS ASSOCIATES

Grace Period Groups - Next Steps

Label a group (Grouper Attributes) with attributes in `control:attr`:

- `ineligibleGroup`: The group to put people in when they fall out ("recently eligible")
- `ineligibleDaysToTrack`: The number number of days for the "grace period" they should have (how long they stay in the "recently eligible" group).
- `preIneligibleGroup`: Group to populate with the static membership of the group, a la "Pre Grace Period" for WebEx
- `formerlyEligibleGroup`: Group to populate with people who were formerly eligible. These people may also be in Grace Period.

Grouper Daemon Loader job in `etc:loader` will read all groups with these labels and (using the service eligibility dates):

- Put people in the "recently eligible" group with an expiration date of sysdate + "grace period" when they are within the grace period window.

Grace Period Groups

Generic version coming to Grouper Community Contributions soon*

Thank You!

*Probably