



UNIVERSITY
of
VIRGINIA

Information Technology Services

The Grouper Chronicles Part 2

Legacy System Challenges at UVA



INTERNET.
2

TECH
ex 24
BOSTON DEC 9-13

“To achieve great things,
two things are needed;
a plan, and not quite
enough time.”

- *Leonard Bernstein*

Flashback:



Lessons Learned about Retiring UVA “MyGroups”

- Grouper went “live” in November ’23 🎉
 - **ONLY** for new groups
- What do we do with these MyGroups?
 - “Refactoring”



New Service Growing Pains

- Running two services led to *a lot* of user confusion.
 - MyGroups behaved differently than Grouper, seen as “simpler” and “easier”
 - Grouper lacked “owner” concept
- Grouper “Business” Service needed work.
 - ServiceNow-based intake process was completely overhauled before we took over MyGroups
- “Operational” vs “Project” work constraints posed a challenge.

Legacy System: MyGroups

- Dates to ca. 2006
 - LDAP reset in 2018
- After initial cleanup still > 15,000 groups
- Lack of governance = massive mess!



MyGroups Analysis

- Imported group objects from AD and LDAP into ElasticSearch
- MyGroup vs. LDAP only groups vs. AD managed groups

LDAP -> AD Member Matching

Huh?

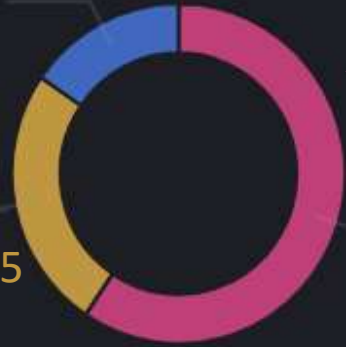
Populations Match!
(Bring into Grouper)

Manual Investigation/Mitigation Needed (15.44%)
2,424

These are in weird places in AD!
(Don't Bring into Grouper)

Not in OU=MyGroups in AD (25.13%)

MyGroups -> Grouper Groups (59.43%)
9,329



“Ancient” (pre-2018) Groups

cn=admin,o=university of virginia,c=us (0.48%)

Active Directory Admin

a.k.a. A real, live human being.

Old AD Service Account

cn=config (39.96%)



If a group hasn't been updated since 2018 by the MyGroups Service Account, we can still import into Grouper, but we hide it and disable any provisioning until someone reaches out!

cn=mygroups-manager,ou=special users,o=university of virginia,c=us (59.54%)

MyGroups Service Account

[+ Request New Group](#)

- Quick links
- My Grouper Groups
 - My Folders
 - My Favorites
 - My Activity
 - Miscellaneous

- Browse Folders/Groups
- UVA
 - Configuration
 - Groups
 - Legacy MyGroups
 - Legacy MyGroups for Biomedical Engineering (BME)
 - Legacy MyGroups for ImageNow
 - Legacy MyGroups for Ivy
 - Legacy MyGroups for SOM Flow Core
 - Legacy MyGroups for ServiceNow
 - Nonprovisioned MyGroups

Home > UVA > Legacy MyGroups

Legacy MyGroups

These groups were originally built in the MyGroups user interface that was retired on 9/17/2024

Show details

Folder contents Privileges More

Enter for: Folder, group, or attribute name

Apply filter Reset

- Name
- Up one folder
 - ADDevelopment
 - AADacts
 - AARRecruit-shared
 - ADWAFindmodules
 - ADStudents
 - ACCMeterns-shared
 - ACLIntervention
 - ACLWorkgroup
 - ADGWGPS
 - ADV-CAL-ChapelParking
 - ADV-CAL-GitPlanning
 - ADV-CAL-OB2428-227
 - ADV-CAL-SARC-FCM
 - ADV-CAL-UAG-OMarketing
 - ADV-CS-14x14x14x14

Grouper Groups: 1,223
(all created since 11/2023)

MyGroups: 7,331

“Other” OUs in AD: 1,201

Non-provisioned: 7,037

About 1k groups have just
been deleted outright.

November 2023 – August 2024 Project Completion	September 2024 Project End	Starting October 2024 Next Steps: Grouper Enhancements
<p>Grouper soft launch employing hybrid model to continue accommodating MyGroups during transition.</p> <p>Moved all users to Grouper for any new group requests.</p>	<p>Grouper becomes official group management platform for UVA.</p> <p>MyGroups is retired.</p> <p>Users are redirected from MyGroups to Grouper and Grouper assumes control of the group.</p> <p>Attestation process in place.</p> <p>Automated groups through Boomi.</p>	<p>API Access to Grouper (through Boomi)</p> <p>Further Automation Enhancements (LSP access to create scripted groups, enhanced Boomi automation data flows)</p> <p>Enhanced Attestation (per-user certification)</p> <p>"Secure" Groups for high-sensitivity access control (e.g. HSVPN enhancements)</p>
<p>Communications: LSP Fall Conference session LSP Digest announcements Updates: MyGroups ITS web page</p>	<p>Communications: LSP Collectives/Conferences LSP Digest New Service Page ITS Web</p>	<p>Communications: LSP Collectives/Conferences LSP Digest</p>

Lessons Learned + Moving Forward

- We lacked adequate transparency with users early in the project.
 - Retiring a service is absolutely terrifying!
- Over-reliance on vendors is bad!
 - Internal data analysis is best done by internal teams.
- Breaking down silos!
 - Once internal groups (“IAM” + “AD” + “LDAP” teams) started working together... magic happened!

Lessons Learned + Moving Forward

- We lacked adequate transparency with users early in the project.
 - Retiring a service is absolutely terrifying!
- Over-reliance on vendors is bad!
 - Internal data analysis is best done by internal teams.
- Breaking down silos!
 - Once internal groups (“IAM” + “AD” + “LDAP” teams) started working together... magic happened!

GROUPER ADVISORY COMMITTEE

SEPTEMBER 5, 2024

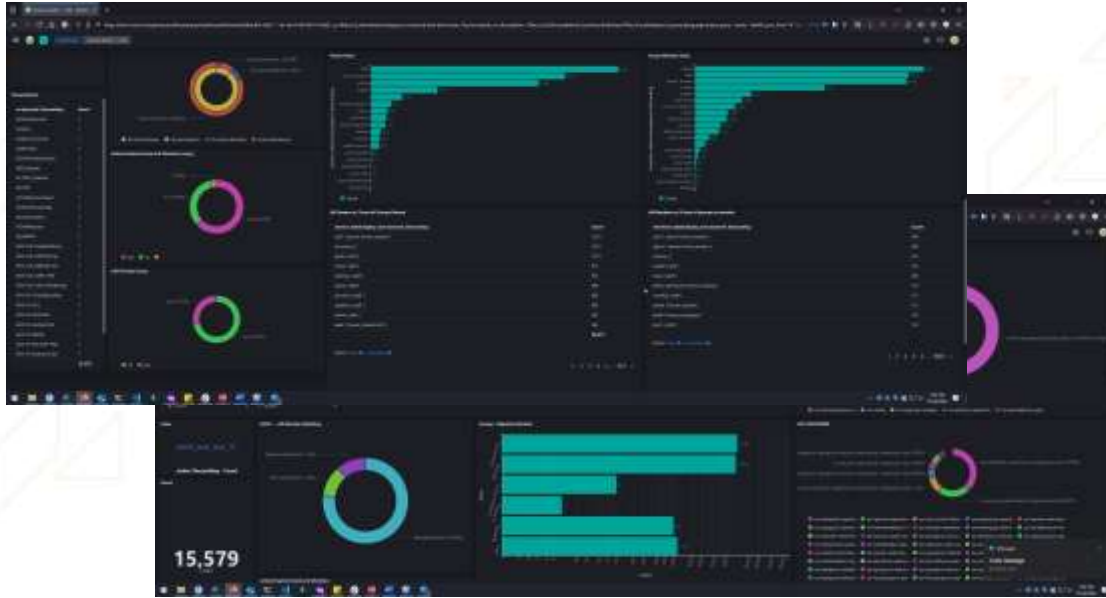


WAH
DOW
AWA
HOO
VAH
DWA

Lessons Learned + Moving Forward

- We lacked adequate transparency with users early in the project.
 - Retiring a service is absolutely terrifying!
- Over-reliance on vendors is bad!
 - Internal data analysis is best done by internal teams.
- Breaking down silos!
 - Once internal groups (“IAM” + “AD” + “LDAP” teams) started working together... magic happened!

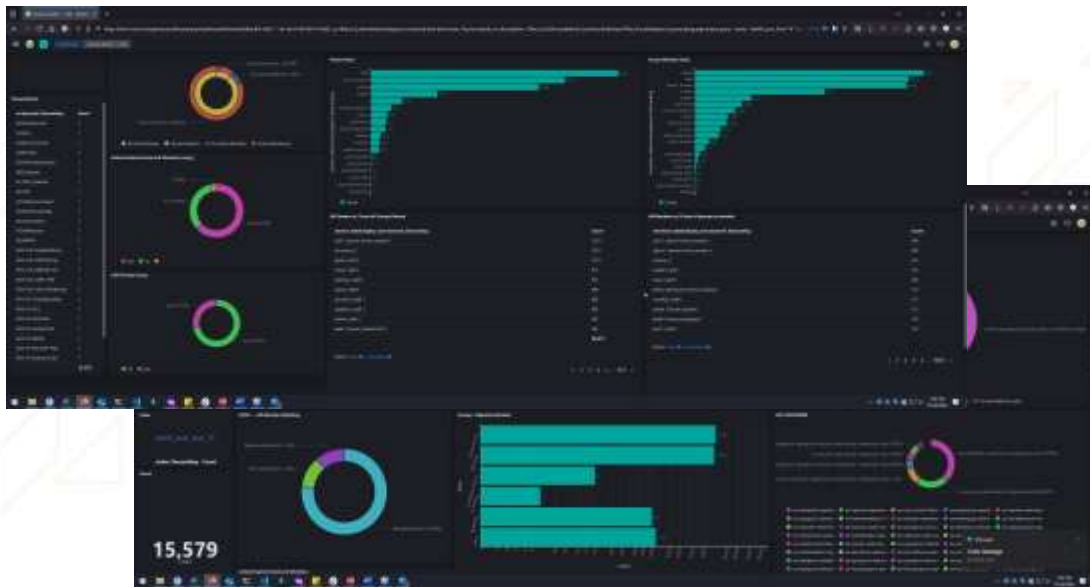
ElasticSearch was Invaluable



- Engineering Insights
 - Provisioners for Non-MyGroups OUs in AD
 - Prioritizing work on different “buckets”
 - What groups can we just outright delete now?

ElasticSearch ~~was~~ Invaluable

is still



– Customer Service

- One stop shop for answering questions about a group...
- “Why can’t I see my MyGroup in Grouper?!”
 - IAM Operations team can look it up without asking IAM Engineering Team

Lessons Learned + Moving Forward

- We lacked adequate transparency with users early in the project.
 - Retiring a service is absolutely terrifying!
- Over-reliance on vendors is bad!
 - Internal data analysis is best done by internal teams.
- Breaking down silos!
 - Once internal groups (“IAM” + “AD” + “LDAP” teams) started working together... magic happened!

INFORMATION TECHNOLOGY SERVICES

as a

STRATEGIC PARTNER

Our People

Be the desired place where people want to work and thrive.

Operational Excellence

Be good stewards of ITS resources, maximize efficiencies, and provide operational excellence.

Research Preeminence

Advance the University's strategy for research preeminence.

Security & Compliance

Create a university-wide culture of shared responsibility and accountability for information security and compliance.

Communicate & Engage

Continually communicate and engage with the University community.

Questions?

Discussion?



Bruce Timberlake – brucetim@umich.edu

Gail Lift – ghl@umich.edu

Liam Hoekenga – liamr@umich.edu

 UNIVERSITY OF MICHIGAN

Kellen Murphy – kellen.murphy@virginia.edu

 UNIVERSITY of VIRGINIA