Centralizing Data using LDAP, SQL and the Web

Jeff Kopmanis, Mathematics IT
kopmanis@umich.edu

October 18, 2006

Numbers

- 300+ Faculty, Graduates and Staff

- 380+ Machines (OSX, Linux, Windows)

- 5 subnets in 3 VLANs

- 3 IT Staff

- 2300+ Undergrad students in lab courses

Solaris Lab Account Creation

- all_classes: Download Classlists from UMIAC (.csv)

- convert_csv: Convert CSV to .create files

- create_account: generate LSA AFS accounts from each .create file

- guardrail: managed /etc/passwd file variations for faculty, lab, staff **user groups**

- guardrail: distributed password files to destination **machine groups**

- All classes took a day to process; Single-user adds took about 10 minutes each; account sheets took 2 days to print!
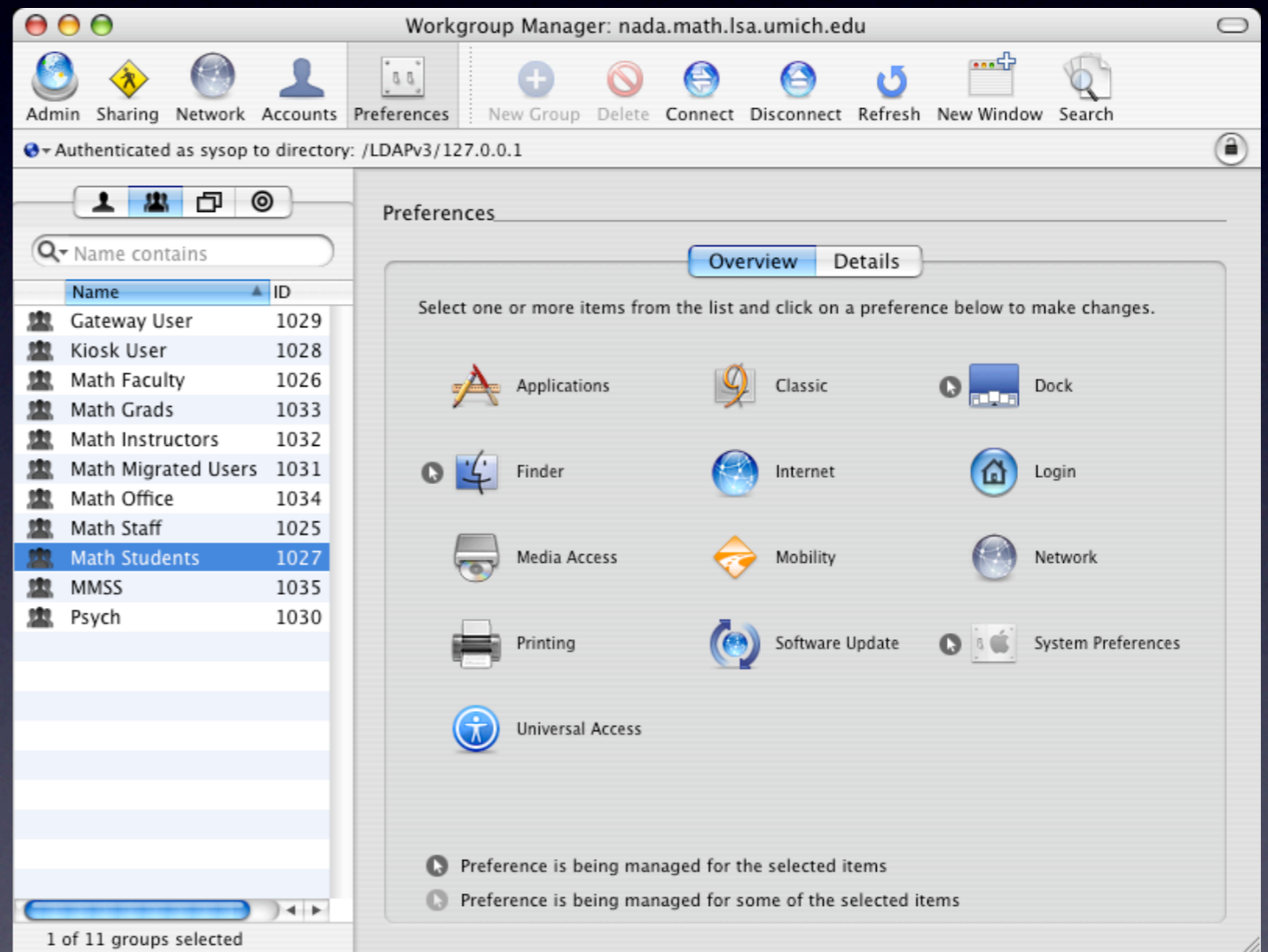
Solaris Lab Account Creation

- all_classes: Download Classlists from UMIAC (.csv)

- convert_csv: Convert CSV to .create files

- create_account: generate LSA AFS accounts from each .create file

- guardrail: managed /etc/passwd file variations for faculty, lab, staff **user groups**

- guardrail: distributed password files to destination **machine groups**

- All classes took a day to process; Single-user adds took about 10 minutes each

Boiled Down:
Capabilities and Permissions

	lab0030	s0137	lab0099	s0237
kopmanis	admin	admin	admin	admin
leonk	grad	grad	grad	grad
jsockolo	student	X	student	X
ronl	X	X	X	X
glarose	faculty	faculty	faculty	admin

June 2003: MacOSX

JXplorer

cn   ▼   =   ▲▼   Quick Search

📄 HTML View   📄 Table Editor

attribute type	value
cn	**B735-EH**
objectClass	apple-computer-list
objectClass	top
apple-computer-list-groups	gateway
apple-computer-list-groups	kiosk
apple-computer-list-groups	mathfaculty
apple-computer-list-groups	mathgrads
apple-computer-list-groups	mathinstructors
apple-computer-list-groups	mathoffice
apple-computer-list-groups	mathstaff
apple-computer-list-groups	mathstudent
apple-computer-list-groups	mmss
apple-computers	lab0203
apple-computers	lab0204
apple-computers	lab0192
apple-computers	lab0144
apple-computers	lab0159
apple-computers	lab0162
apple-computers	lab0183
apple-computers	lab0152
apple-computers	lab0184
apple-computers	lab0128
apple-computers	lab0142
apple-computers	lab0166
apple-computers	lab0133
apple-computers	lab0149
apple-computers	lab0141
apple-computers	lab0140
apple-computers	lab0250

Explore   🔍 Results   ▶

World
- ● edu
  ▼ ● umich
    ▼ ● lsa
      ▼ ● math
        ▶ accesscontrols
        ▶ autoserversetup
        ▶ certificateauthoritie
        ▼ computer_lists
          ▶ 1st Floor
          ▶ 1st Floor Offices
          ▶ 2nd Floor
          ▶ 2nd Floor Office
          ▶ 3rd Floor
          ▶ 3rd Floor Office
          ▶ 4th Floor
          ▶ 4th Floor Office
          ▶ 5th Floor
          ▶ 5th Floor Office
          ▶ B069-EH
          ▶ B723-EH
          ▶ B727-EH
          ▶ B728-EH
          ▶ B735-EH
          ▶ B737-EH
          ▶ B743-EH
          ▶ B745-EH

Submit   Reset   Change Class   Properties

Connected To 'ldap://nada:389'

2003 Account Creation

- Everything from the Solaris procedures, except...
  - No more LSA AFS home dirs to create
  - UMICH Kerberos, aka "Single sign-on" (No more account sheets!)
- test_ldap.pl: load LDAP from lab password file
- All classes take about 2 hours to process; Single-user adds took about 10 minutes each; LDAP load adds only 30 seconds
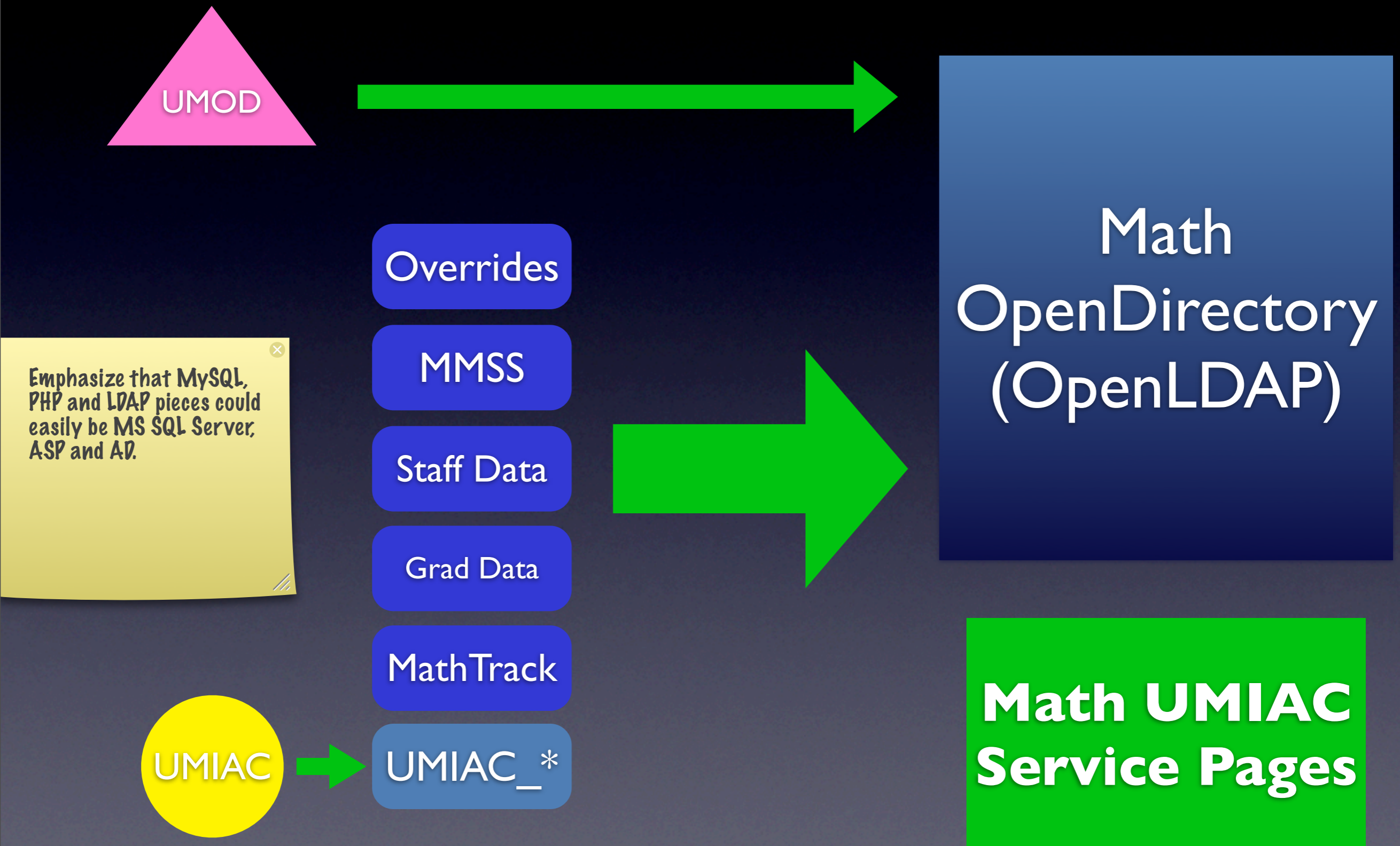- 2000+ Undergrad students in lab courses

2003 Account Creation

- Everything from the Solaris procedures, except...

  - No more LSA AFS home dirs to create

  - UMICH Kerberos, aka "Single sign-on" (No more account sheets!)

- test_ldap.pl: load LDAP from lab password file

- All classes take about **2 hours** to process; Single-user adds took about **10 minutes** each; LDAP load adds only **30 seconds**

- 2000+ Undergrad students in lab courses

Solaris "Sunset"

August 15, 2006 is the proposed shutdown

But...we now have no capacity to build sources

Data Flow

UMOD

Overrides

MMSS

Staff Data

Grad Data

MathTrack

UMIAC → UMIAC_*

Math OpenDirectory (OpenLDAP)

Math UMIAC Service Pages

Emphasize that MySQL, PHP and LDAP pieces could easily be MS SQL Server, ASP and AD.

Admin | Sharing | Network | Accounts | Preferences | New Computer List | Delete | Connect | Disconnect | Refresh | New Window | Search

Authenticated as sysop to directory: /LDAPv3/127.0.0.1

List | Access | Cache | Inspector

Name contains

Name
1st Floor
1st Floor Offices
2nd Floor
2nd Floor Offices
3rd Floor
3rd Floor Offices
4th Floor
4th Floor Offices
5th Floor
5th Floor Offices
B069-EH
B723-EH
B727-EH
B728-EH
B735-EH
B737-EH
B743-EH
B745-EH
MathIT
REU Lab

1 of 23 lists selected

○ All groups can use the computer
● Restrict to groups below

Name	ID
Gateway User	1029
Kiosk User	1028
Math Faculty	1026
Math Grads	1033
Math Instructors	1032
Math Office	1034
Math Staff	1025
Math Students	1027
MMSS	1035

+
−

☑ Allow users with local-only accounts
☑ Local-only accounts pick workgroups from the above list (OS 10.4 clients and later only)
☑ Allow computer administrators to disable management (OS 10.4 clients and later only)

Presets: None

Revert | Save

Why Mirror in MySQL?


```
                    JOIN od_cross_listed ON courses_taught.course=od_cross_listed.mcrs)";
$odresult = mysql_query( $odsql ) or die("There was an error creating od_xlist_tmp: ".mysql_error()."<br>\n");

## Generate the list of uniqnames to add to the mathstudent group
## WARNING: be careful about Lab/Lecture issues with respect to duplicate rows!
$math_sql = "(SELECT DISTINCT math.umiac_classlists.uniqname as uniqname
                FROM od_xlist_tmp
              LEFT JOIN math.umiac_classlists ON od_xlist_tmp.course = math.umiac_classlists.course
                  AND (od_xlist_tmp.section = math.umiac_classlists.section OR od_xlist_tmp.section = '*')
              LEFT JOIN math.umiac_sections ON od_xlist_tmp.course = math.umiac_sections.course
                  AND (od_xlist_tmp.section = math.umiac_sections.section OR od_xlist_tmp.section = '*')
               WHERE ( status = 'Student' ))
                 UNION DISTINCT
             (SELECT DISTINCT uniqname FROM math.overrides WHERE expires>=curdate() AND (ldapGrp = 'mathstudent' OR ldapGrp = '*'))
                 UNION DISTINCT
             (SELECT DISTINCT uniqname FROM math.math_reu)
                 UNION DISTINCT
             (SELECT DISTINCT uniqname FROM math.math_majors)
                 UNION DISTINCT
             (SELECT DISTINCT uniqname FROM math.staff)
                 ORDER BY uniqname";
  $math_result = mysql_query( $math_sql ) or die( "There was an error: ".mysql_error()."<br>\n");
  while( $mathdata = mysql_fetch_array( $math_result )) {
     $math_arr[$i] = $mathdata[uniqname];
     ++$i;
  }
}


function instructor_sql_search( &$instructor_arr ) {
  $i = 0;
  $instructor_sql = "(SELECT DISTINCT math.umiac_classlists.uniqname as uniqname
                        FROM math.courses_taught LEFT JOIN math.umiac_classlists
                        ON  math.courses_taught.course = math.umiac_classlists.course
                        WHERE ( status = 'Instructor' ))
                          UNION DISTINCT
                        (SELECT DISTINCT uniqname FROM math.overrides WHERE expires>=curdate() AND (ldapGrp = 'mathinstructors' OR ldapGrp
= '*'))
                                                                                                                    124,20        31%
```

Special Circumstances: Overrides

kopmanis@db1.math.lsa.umich.edu/math (MySQL 4.0.24_Debian-10sarge2-log)

Show Console | Clear Console | Show Variables | Flush Privileges | Optimize Table | Create Table Syntax

Databases

math

Tables

- math_majors
- math_reu
- od_cross_listed
- od_web_counters
- od_xlist_tmp
- overrides
- platform_survey
- repTheory_register
- sitc_sched
- softserv
- staff
- submerge_app
- tblFaculty
- tblFacultyResearchArea
- tblOfficeStaff
- umiac_classlists
- umiac_courses
- umiac_sections
- weeklyExceptions

Encoding

Structure | Content | Custom Query | Dumps

name | is | | Search | Show All

No limit | | Go

name	uniqname	ldapGrp	comment	id	expires
Richard White	rjacobw	*	Student Author	1	2099-12-31
Jeff Kopmanis	kopmanis	*	The big boss	2	2099-12-31
NULL	mcglam	mathstudent	463 override	30	2099-12-31
NULL	gornickm	mathstudent	NULL	12	2006-09-01
NULL	apmiller	mathstudent	NULL	13	2006-09-01
Paul Federbush	pfed	mathfaculty	emeritus	14	2099-12-31
NULL	iadeboye	mathgrads	grad	15	2006-09-01
NULL	wlorenz	mathgrads	grad	16	2006-12-31
Sato Kentaro	kensato	mathfaculty	Visiting Scholar	31	2099-12-31
NULL	ibragim	mathfaculty	Visitor in 3864	29	2007-01-01
NULL	robertka	mathfaculty	Visitor in 2867	28	2099-12-31
NULL	jmwu	mathfaculty	Visitor in 4071	27	2099-12-31
NULL	laustin	mathstudent	NULL	26	2099-12-31
NULL	tding	mathstudent	NULL	25	2099-12-31
NULL	klogan	mathstudent	NULL	24	2099-12-31
NULL	grusso	mathfaculty	Visitor of	23	2006-12-31
NULL	sonmez	mathfaculty	Visitor in 4823	22	2006-08-31
NULL	lapierap	mathstudent	fulfilling	32	2006-12-31
NULL	noahf06	mathstudent	HS override	33	2006-12-25
NULL	kensato	mathstudent	ablass guest	34	2099-12-31
NULL	mguest	mathstudent	Math Guest	35	2099-12-31

21 rows in table

Which courses to populate?

Demo

Moving Forward

- Common LDAP repository built on live data

- Mirrored MySQL tables to data-mine with existing data

- New data sources add to our capabilities

- Web updates planned for F06/W07 to streamline usage, eliminate need for MySQL tool (CocoaMySQL, phpMyAdmin)

Gateway Testing

- ITC project can now use pam_ldap to authorize against our directory

- No more local accounts - UMICH Kerberos

- Automated exam assignments

- Late-adds and exceptions are no longer a problem

Grad Student Evaluations

- Currently, requires an Oracle SQL query to the MAIS data, which generates an Excel .xls file.

- Math staff import this to MySQL.

- Eval forms are web-based and generated from the MySQL tables and MathTrack data.

- With Instructors in UMIAC data, we can eliminate a 2-step human process, and get the data directly, and error-free.

NetBoot Ethernet Filters

- Auto-populate NetBoot ethernet filters from NetReg data

- eliminates triple-entry of data and increases accuracy of LDAP data

- All ethernet devices can be "registered"

Machine Locations

- Tie into LSAIT NetReg MySQL database (read-only)

- Use Dept field for uniqname and room

- eliminates triple-entry of data

- Auto-populate existing LDAP machine groups from NetReg data (eg. B745, B735, etc)

- New: manage ALL machines by location

Apple Remote Desktop

- A script to wrap ARD binary

- script would auto-generate admin plists

- generated plists would contain only the machines currently in that lab

"Live" Inventory

- Every functioning machine from NetReg

- Extra fields can be JOINed in SQL

- If NetReg is accurate, we get accurate inventory for free

Status Reports

- Find machines associated with faculty or staff member

- Recover IPs from personal laptops once the person has left the department

- Easier to recover IPs from machines no longer in the department (Dispo, loss, etc)

Benefits of NetReg Use

- NetReg becomes an integral part of our administrative systems

- Streamlines entry of machines into the department

- Eliminates redundant entry of ethernet addresses

Links

OpenLDAP
http://www.openldap.org

PHP LDAP Functions
http://us3.php.net/manual/en/ref.ldap.php

LDAP Query Basics from Visual Basic
http://rulink.rutgers.edu/ldap-vb.html

Active Directory LDAP Query Basics
http://www.microsoft.com/technet/prodtechnol/exchange/2003/insider/ldapquery.mspx

MySQL Reference Manual
http://dev.mysql.com/doc/refman/5.0/en/index.html

Jeff Kopmanis, IT Supervisor, Mathematics
kopmanis@umich.edu