



A Middleware Unified Field Theory

Identity Management / Directories

Privileges / Groups

Single Sign-On / Federation

Diagnostics

Enterprise Integration

from network to application

Michael R Gettes
Internet2
November 2007

What do we want?

Inter-Enterprise Workgroup Collaborations

not sexy

or

Collaborative
Organizations

CO

Identity

Groups

Privileges

Federated Access

and ...

Applications

“It’s the App stupid!”

Give

COntrol

To

COmmunity Members

Integrate with
Existing
COmmon
IT Infrastructures
in
Higher Education

Flexible
Scalable
Modular



COmponents

SHIBBOLETH

Identity
Mgr

Signet

Grouper

C
O

LDAP
Directory

LDAP-PC

Applications & Network

stop talking
start walking

demo

COmanage.internet2.edu

COmponents

SHIBBOLETH

Identity
Mgr

Signet

Grouper

C
O

LDAP
Directory

LDAP-PC

Applications & Network

Comanage ...

is only a demonstration of
the CO model

*a CO fits within a service
delivery strategy*

Stuff stored in Directories

(everybody has one)

Directories make
Priv/Group data more
accessible

Application Management

App Access to data is
managed by LDAP (initially)

Identity data can be distributed by any desired mechanism in the future. SQL databases, feeds, message bus technologies.

Truth be told...

LDAP-PC

Large-Scale Performance and namespaces

SIGNET

Minor UI and Deployment

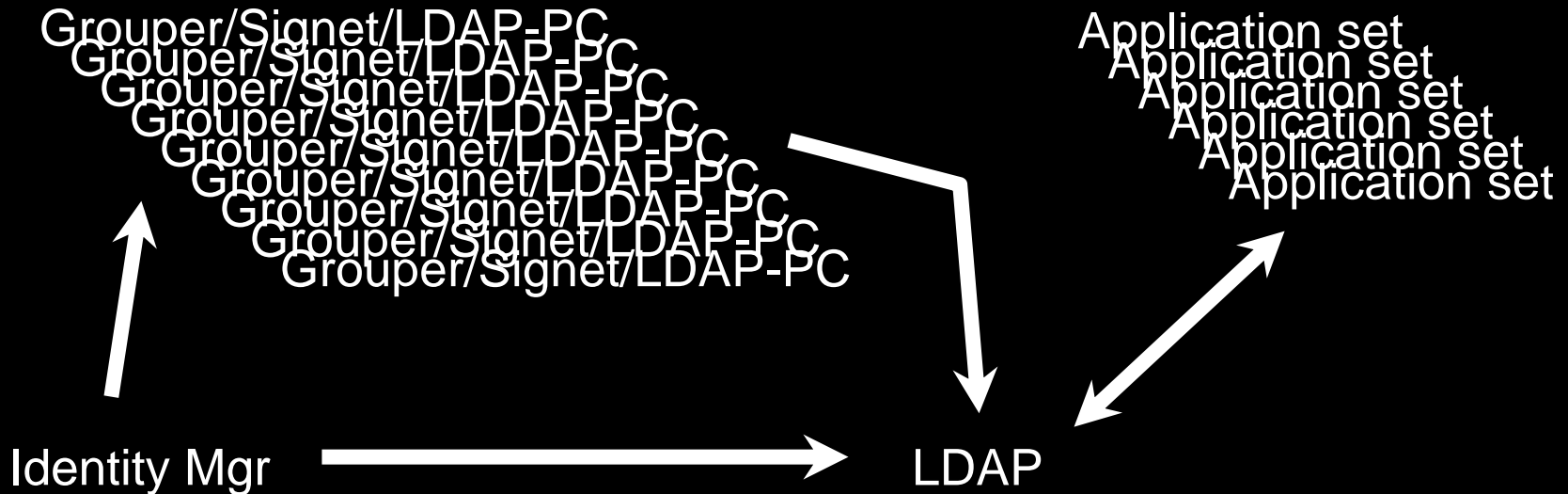
GROUPE

Some UI and Large-scale Performance

SIGNET only immediate concern

Many COs on a single server

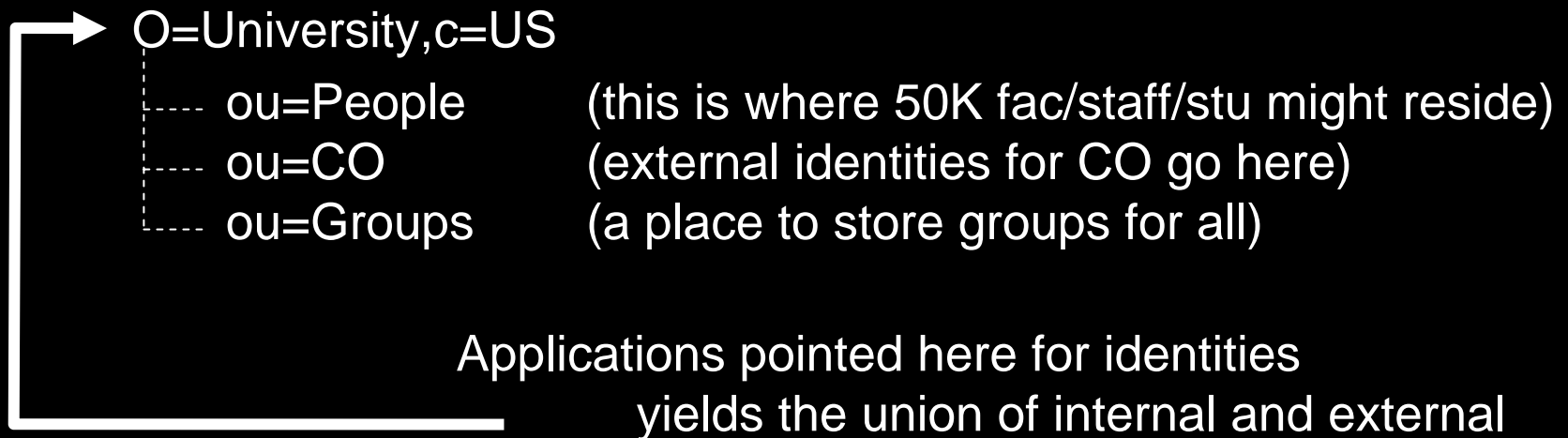
(if you wanna do that)



No local identity issued for external users to access CO services

big win!

Example directory tree for CO environment



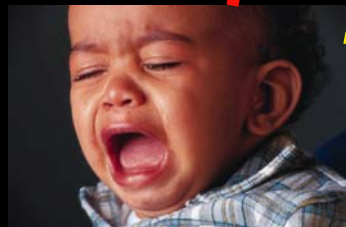
Future...

Begin addressing issues of “attribute
eCOonomy”

Protect CO by Identity Provider...

can solve “IEEE problem”?

Web site
wants to
know:
Are you a
member
of IEEE?



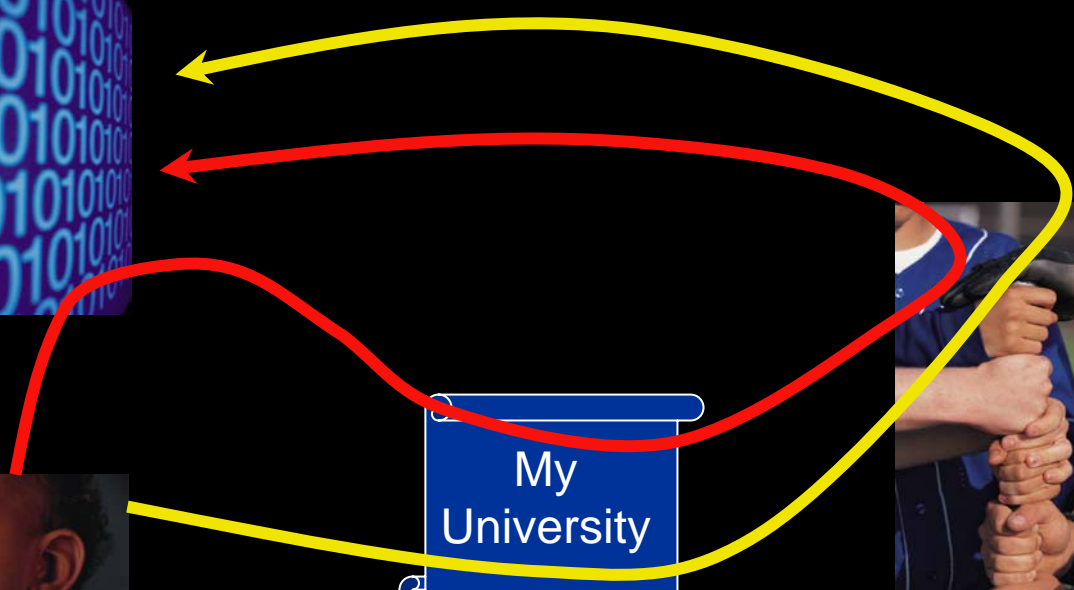
User



Home
Identity Provider



IEEE-CO
This org has
membership
data but does
not manage
identity - a CO
with only
external users.



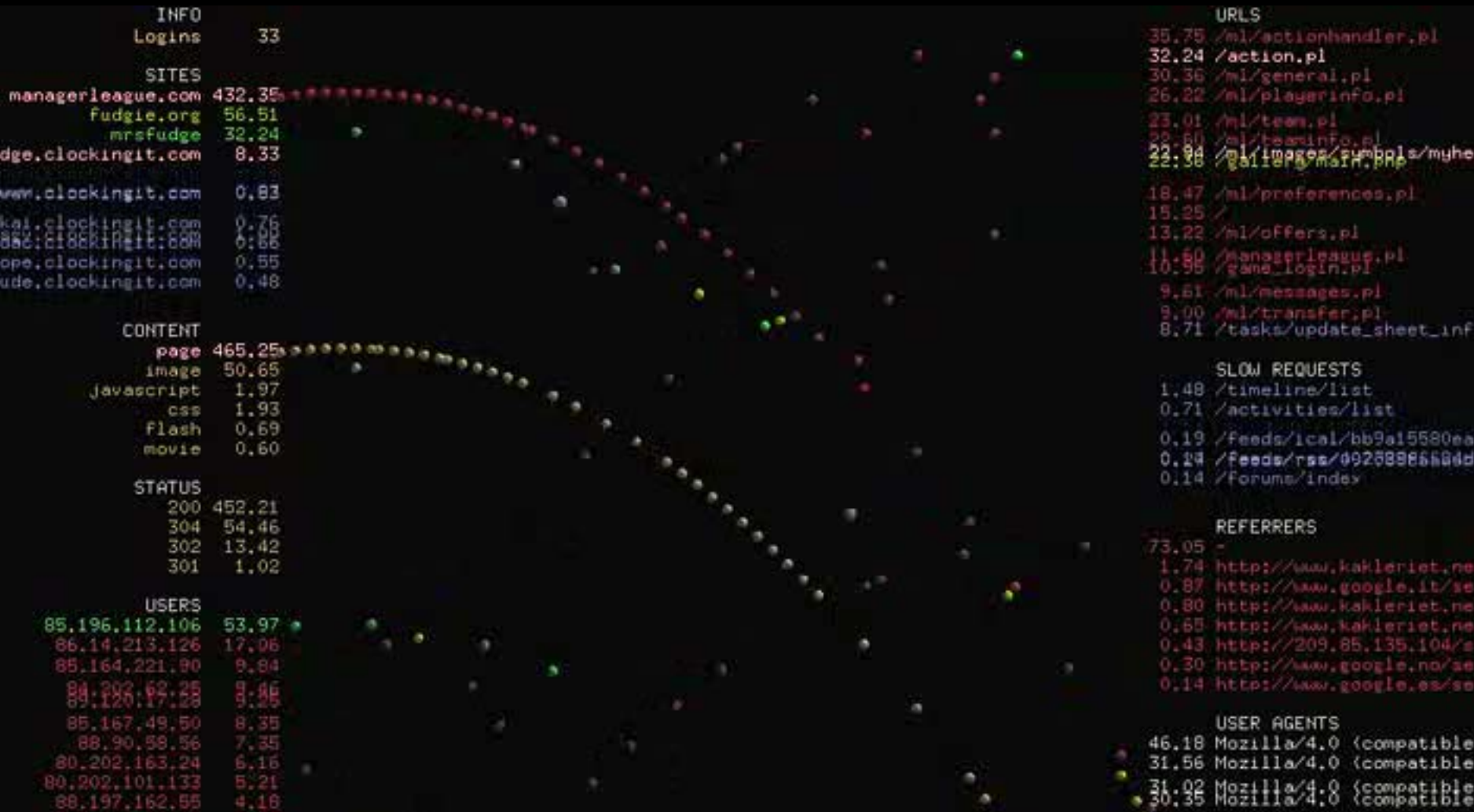
Diagnostics

*Lifting up shib log files
and making EDDY deposits*

Creating a unified and federated view of diag data

- Network data: flows, snort, snmp
- System stats: cpu, i/o, mem, etc...
- Infrastructure: shib, ldap, authN, etc...
- Application: http, confluence, sympy, calendar
etc, etc, etc...

<http://web.cmu.edu/eddy>



INFO				URLS	
Logins	33			35.75	/ml/actionhandler.pl
SITES				32.24	/action.pl
managerleague.com	432.35			30.36	/ml/general.pl
fudgie.org	56.51			26.22	/ml/playerinfo.pl
mrsfudge	32.24			23.01	/ml/team.pl
dge.clockingit.com	8.33			22.60	/ml/teaminfo.pl
www.clockingit.com	0.83			22.98	/ml/images/symbols/myhe
kai.clockingit.com	0.76				/ml/images/main.png
880:ci880R8it:880	0.66			18.47	/ml/preferences.pl
ope.clockingit.com	0.55			15.25	/
ude.clockingit.com	0.48			13.22	/ml/offers.pl
CONTENT				11.60	/managerleague.pl
page	465.25			10.95	/game_login.pl
image	50.65			9.61	/ml/messages.pl
javascript	1.97			9.00	/ml/transfer.pl
css	1.93			8.71	/tasks/update_sheet_inf
flash	0.69			SLOW REQUESTS	
movie	0.60			1.48	/timeline/list
STATUS				0.71	/activities/list
200	452.21			0.19	/feeds/ical/bb9a15580ea
304	54.46			0.14	/feeds/rss/0925898666dd
302	13.42			0.14	/forums/index
301	1.02			REFERRERS	
USERS				73.05	-
85.196.112.106	53.97			1.74	http://www.kakleriet.no
86.14.213.126	17.06			0.87	http://www.google.it/se
85.164.221.90	9.84			0.80	http://www.kakleriet.no
88.202.62.25	8.46			0.65	http://www.kakleriet.no
89.120.17.29	8.25			0.43	http://209.85.135.104/s
85.167.49.50	8.35			0.30	http://www.google.no/se
88.90.58.56	7.35			0.14	http://www.google.es/se
80.202.163.24	6.16			USER AGENTS	
80.202.101.133	5.21			46.18	Mozilla/4.0 (compatible)
88.197.162.55	4.18			31.56	Mozilla/4.0 (compatible)
				30.92	Mozilla/4.0 (compatible)
				30.35	Mozilla/4.0 (compatible)

Network Layer?

Why not?

Integrate with Grids?

Why not?

Addresses VO scenarios?

Why not?

VOC?



it's all about /me

done

<http://middleware.internet2.edu/co>

Talk amongst yourselves