

# Directory Operations It's Getting Deeper

Internet2 Middleware Early Adopters Workshop  
March, 2000

Michael R. Gettes  
Lead Application Systems Integrator  
Georgetown University  
gettes@Georgetown.EDU

# Site Profile

## dc=Georgetown,DC=EDU

- Netscape/iPlanet DS version 4.11
  - 2 Sun E250 dual cpu, 512MB RAM
- 65,000 DNs (25K campus, others = alums + etc)
- Directory + apps implemented in 6 months
- Distinguished names: uid=x,ou=people
  - DC rant? Where is Bob Morgan when you need him?
- NSDS pre-op plugin (by gettes@Princeton.EDU)
  - Authentication over SSL; Required
  - Can do Kerberos – perf problems to resolve
- 1 supplier, 4 consumers

# Applications

- Mail routing with Sendmail 8.10 (lists also)
- Netscape messaging server v 4.15 (IMAP)
  - WebMail profile stored in LDAP
- Apache web server for Netscape roaming
- Apache & Netscape enterprise web servers
- Blackboard CourseInfo enterprise edition
- Whitepages: directory server gateway
- DSGW for priv'd access and maintenance

# Applications (Continued)

- Remote access with RADIUS (funk).
  - No SSL or proper LDAP binding (as of 3/2000).
  - Authenticates and authorizes for dial-up, DSL and VPN services using RADIUS called-id.
- Alumni services (HoyasOnline).
  - External vendor in Dallas, TX (PCI).
  - They authenticate back to home directories. Apache used to authenticate and proxy to backend IIS server.

# Applications (Continued)

- Specialized support apps
  - Self service mail routing
  - HD: mail routing, password resets, quota management via DSGW
  - Change password web page
- Person registry populates LDAP people data, currently MVS based.
- PerLDAP used quite a bit – very powerful!

# Applications (Continued)

- Georgetown Netscape communicator (CCK).
  - Configured for central IMAP/SSL and directory services.
  - Handles versions of profiles.
- Future: more apps! Host DB, Kerberos integration, win2k/ad integration?, Automatic lists, Dynamic/static Groups.

# General Operational Controls

- Size limit trolling (300 or 20 entries?)
- Lookthru limit (set very low)
- Limit 3 processors for now, MP issues still!
- 100MB footprint, about 8000 DNs in cache
- 24x7 operations
- What can users change?? (Very little)
- No write intensive applications

# General Ops Controls

- Anonymous access allowed

# Schema: Design & Maint

- Unified namespace: there can be only one!
- Schema design and maintenance
  - Space/time tradeoffs on indexing
  - Edu-person 0.9 vs. guPerson
  - guRestrict, guEmailBox, guAffil, guPrimAfil
  - guPWTimebomb, guRadProf, guType, guSSN
  - Relationships (guref)
- Maintained by file using ldapmodify

# Access Lists: Design & Maint

- Access lists: design & maintenance
  - Buckley(FERPA) protection & services
  - Priv'd users and services
  - userPassword & SSN
- Maintained by file using ldapmodify
- Working on large group controls now

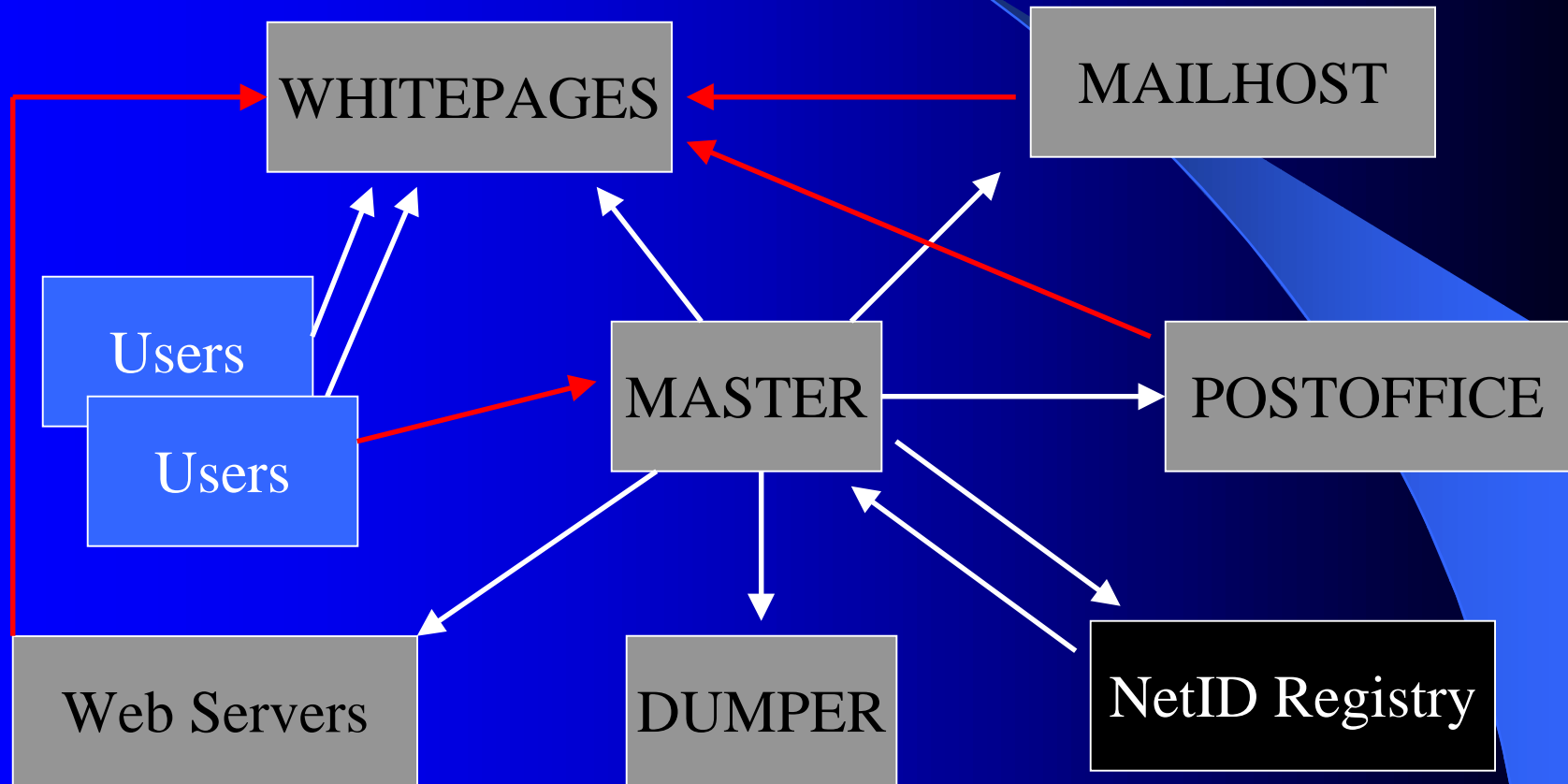
# Replication

- Application/user performance
- Failover, user and app service
- Impact of DC= naming (replica init)
- Monitoring: web page and notification
- Dumper replica – periodic LDIF dumps
- Backups? We don't need no stinkin' backups!
  - No good solution for backups

# Replication (Continued)

- Application/users config for mult servers
- Deterministic operations vs random
- Failover works for online repairs
- Config servers are replicated also
- 10 to 1 SRA/CRA ratio recommended
- Cannot cascade with DC=
  - Cascading is scary to me

# Data/Replica Structure



# Other Directories

- Novell – abandoning GroupWise. Will likely abandon NDS due to support and perspective.
- Active directory??? Ugh!!!
- Integrate whitepages service with hospital.

# Netscape Console

- Java program (FAT client).
- Used to create, configure and monitor Netscape servers.
- Preferred the web page paradigm of the version 3 products.
- Has enough bugs that it is only used by server admins, not for mere mortals.
- Demo???

# Directory of Directories

- Outgrowth of Georgetown WhitePages.
- Exposes common schema issues. Edu-person 0.9.
- Performance issues for massively parallel searches.
- Interesting lessons learned about LDAP API.
- Working with iPlanet/Netscape to use DSGW for this project.