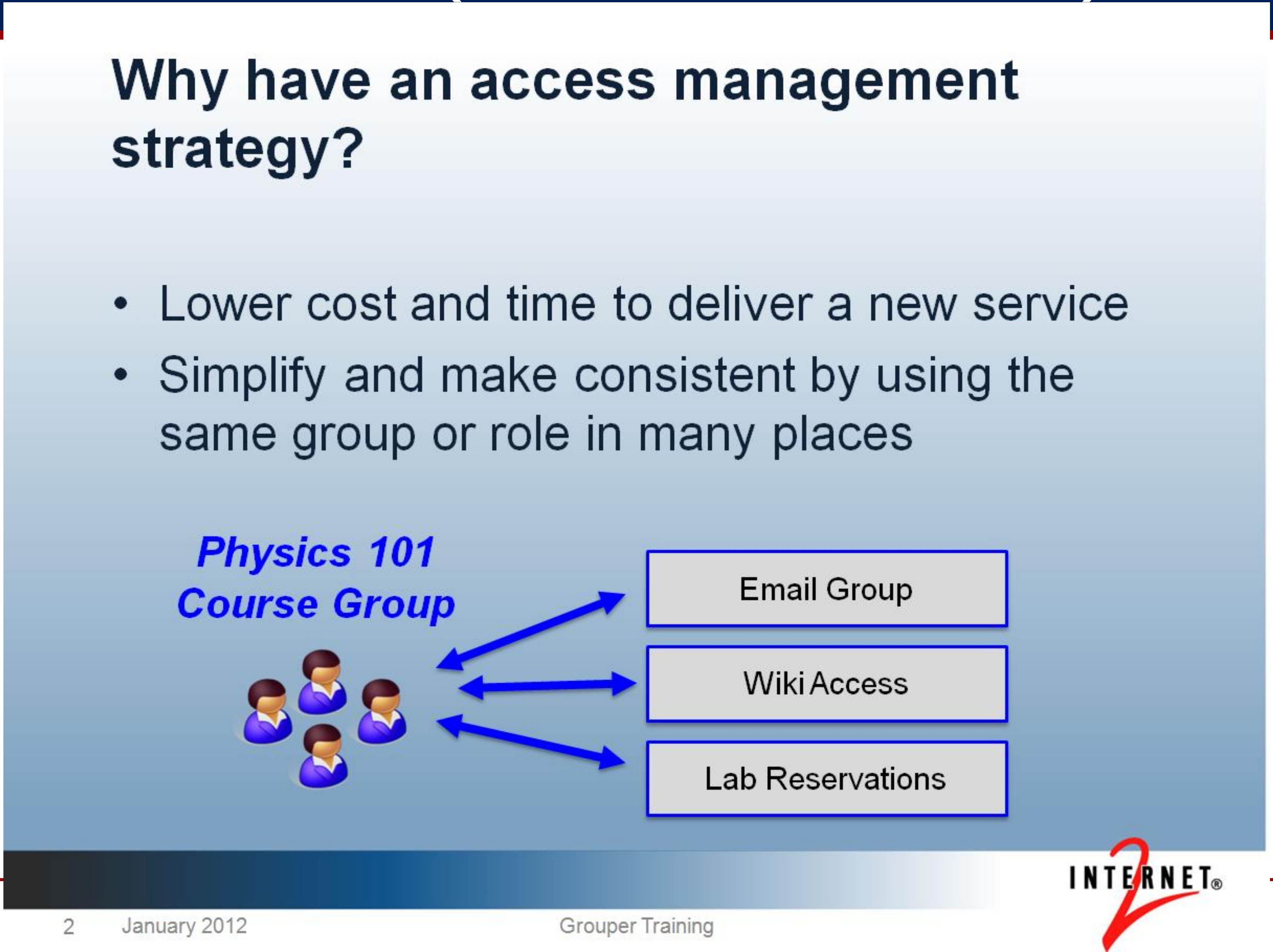
# PennGroups Intro / HA / UI

May 2014

# Agenda

- Introduction to PennGroups (Grouper)
- Recent use cases
- Recent improvements in availability
  - Architecture
  - Client failover between WS and LDAP
  - New readonly WS server offsite
  - DNS failover for readonly WS
  - Client failover between WS onsite and offsite
- New UI
  - Description
  - Bake-off

# Introduction (slides borrowed)



## Why have an access management strategy?

- Lower cost and time to deliver a new service
- Simplify and make consistent by using the same group or role in many places

*Physics 101 Course Group*

Email Group

Wiki Access

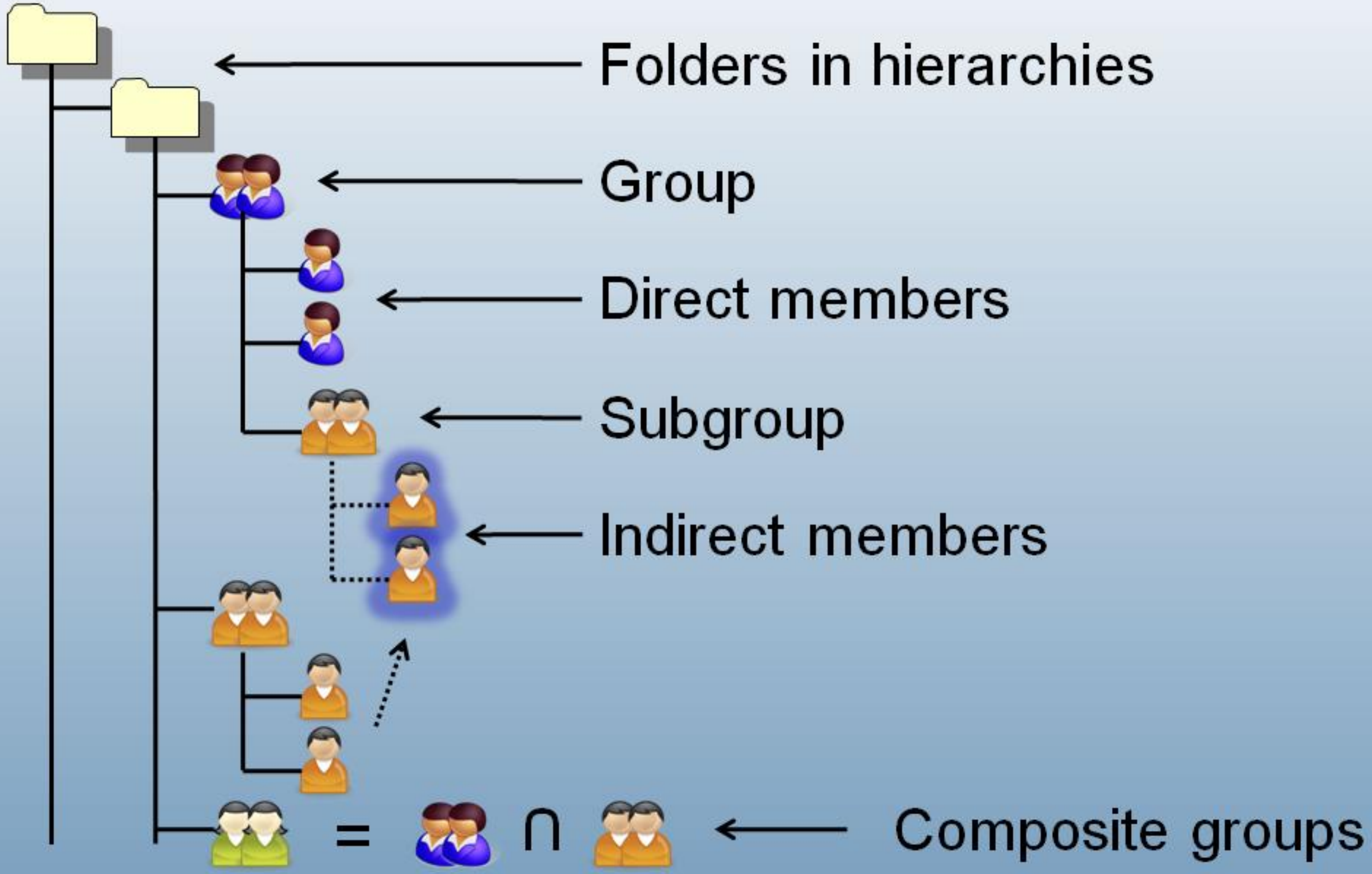
Lab Reservations

# Additional benefits of access management

- Empower the right people to manage access. Take central IT out of the loop.

- See who can access what, with a report rather than a fire drill

# Grouper: core concepts



Folders in hierarchies

Group

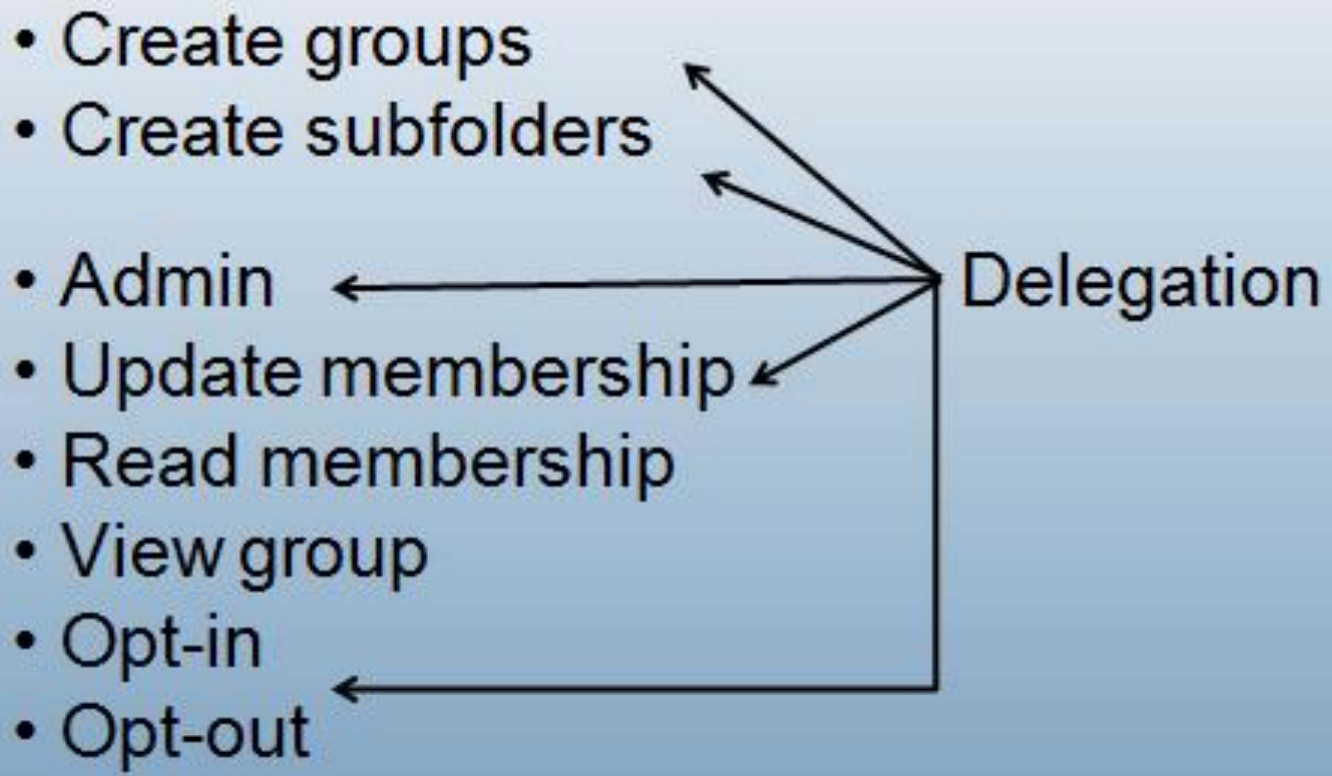
Direct members

Subgroup

Indirect members

Composite groups

# Security & delegation

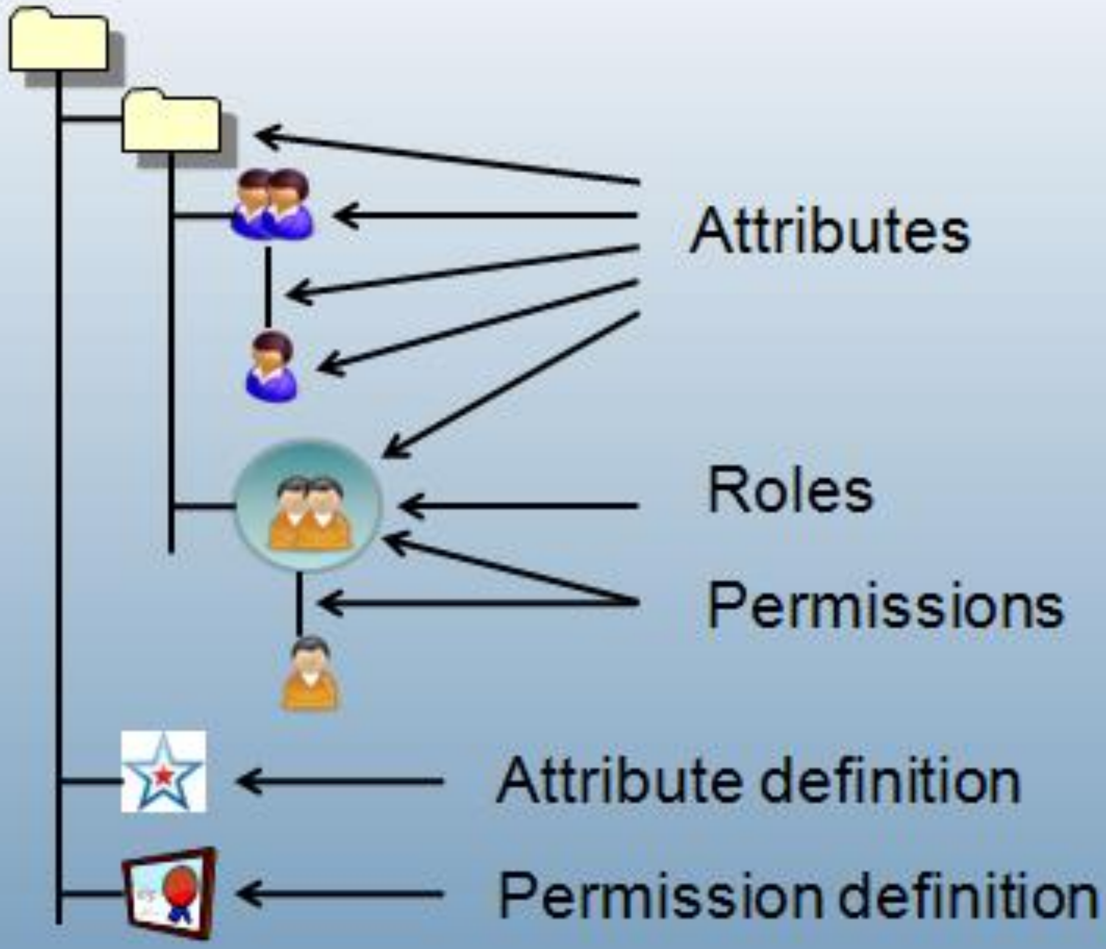


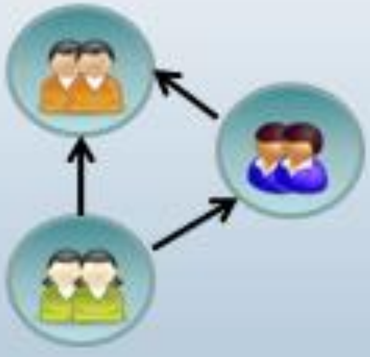
- Create groups
- Create subfolders

- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

Delegation

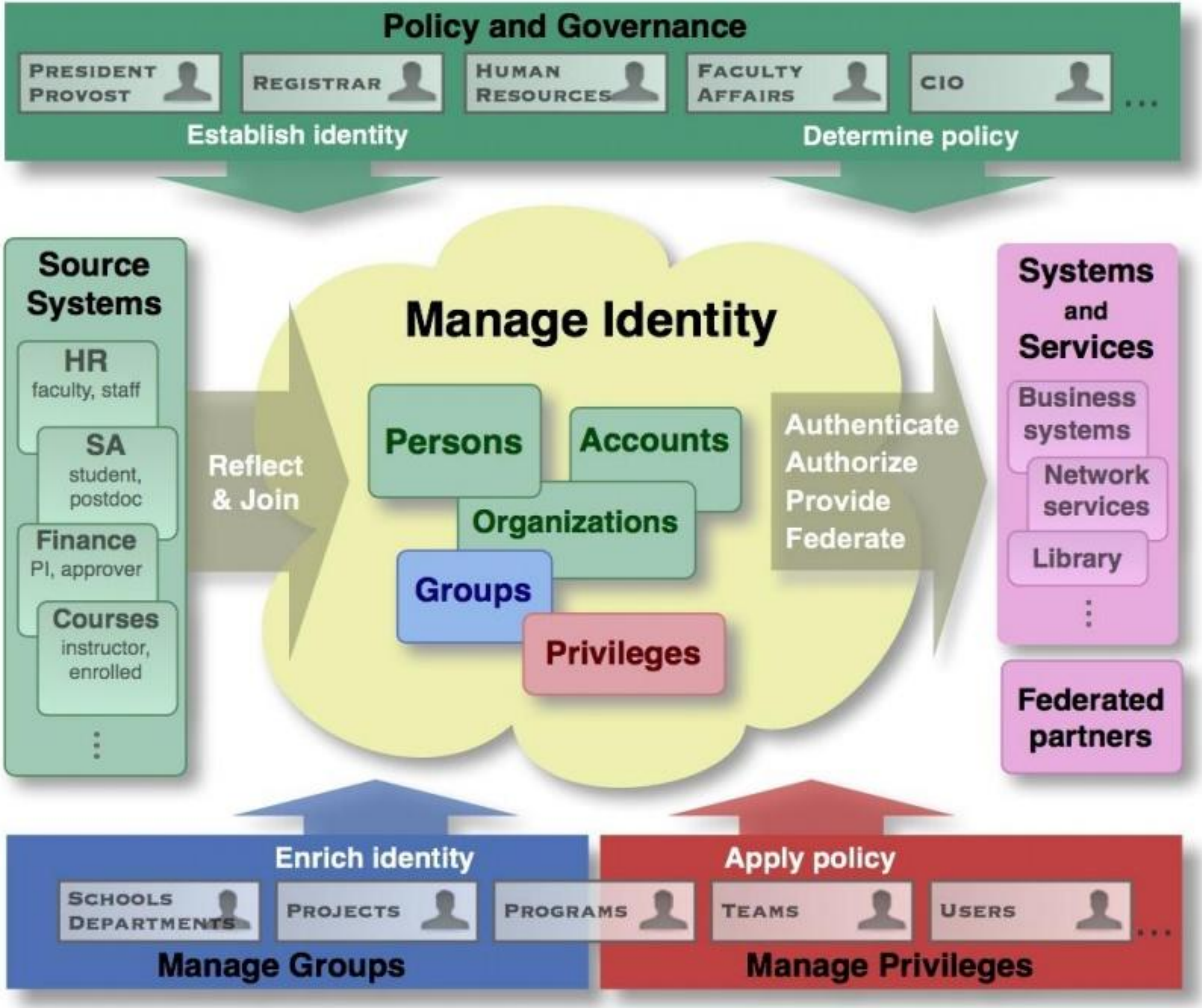
# Beyond groups





Role inheritance

Delegation model extends that for Groups



Policy and Governance

PRESIDENT PROVOST

REGISTRAR

HUMAN RESOURCES

FACULTY AFFAIRS

CIO

…

Establish identity

Determine policy

Source Systems

HR
faculty, staff

SA
student, postdoc

Finance
PI, approver

Courses
instructor, enrolled

⋮

Reflect & Join

Manage Identity

Persons

Accounts

Organizations

Groups

Privileges

Authenticate
Authorize
Provide
Federate

Systems and Services

Business systems

Network services

Library

⋮

Federated partners

Enrich identity

Apply policy

SCHOOLS DEPARTMENTS

PROJECTS

PROGRAMS

TEAMS

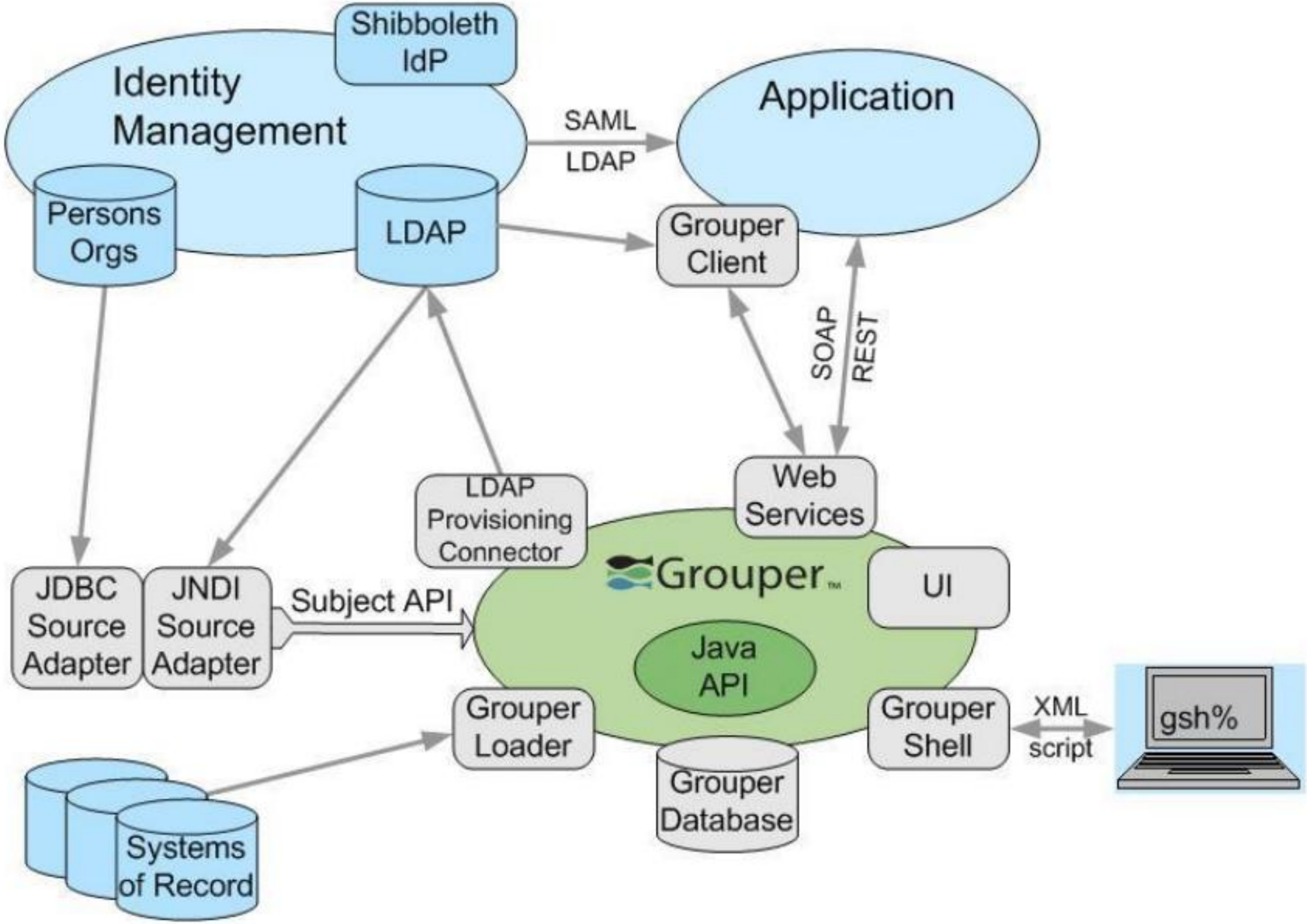
USERS

…

Manage Groups

Manage Privileges

# Grouper integration



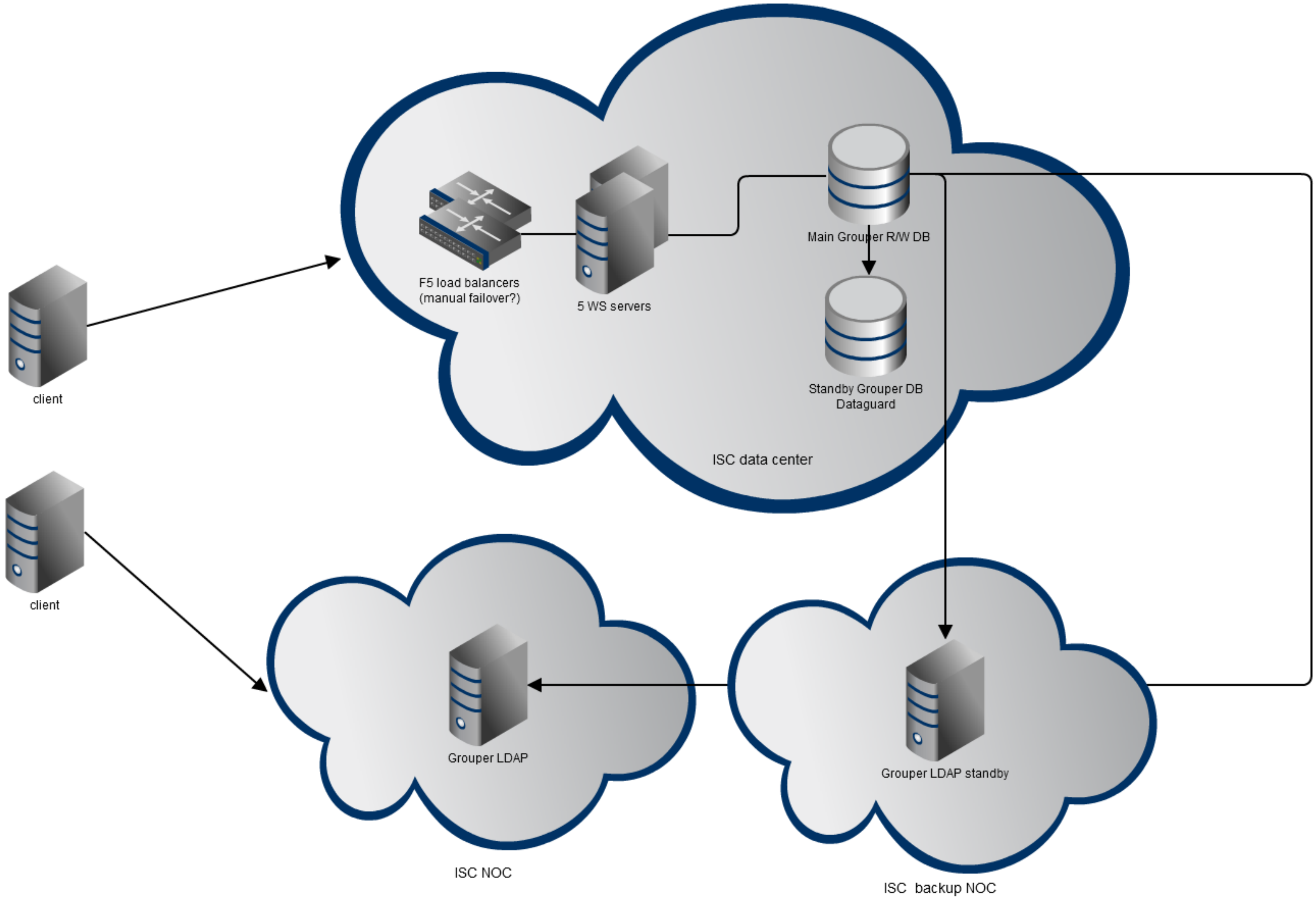
# Recent use case - Canvas

- Needed to lock out half of the users of canvas during maintenance
- Created two large ad hoc groups by importing CSV’s of pennids or pennkeys
- The WebLogin team configured Shibboleth to make this happen based on the group
- The service owners could edit the group memberships

# Recent use case – License change

- An application needed to change its user base
- Used to be all IT staff
- Now should be IT staff minus 3 centers
- Orgs and centers were previously loaded into grouper
  - Created a new overall group for application
  - Marked it as “include/exclude” type
  - Added itstaff to the includes
  - Added 3 centers to excludes
  - The WebLogin team changed the application Shibboleth configuration to point to the new group

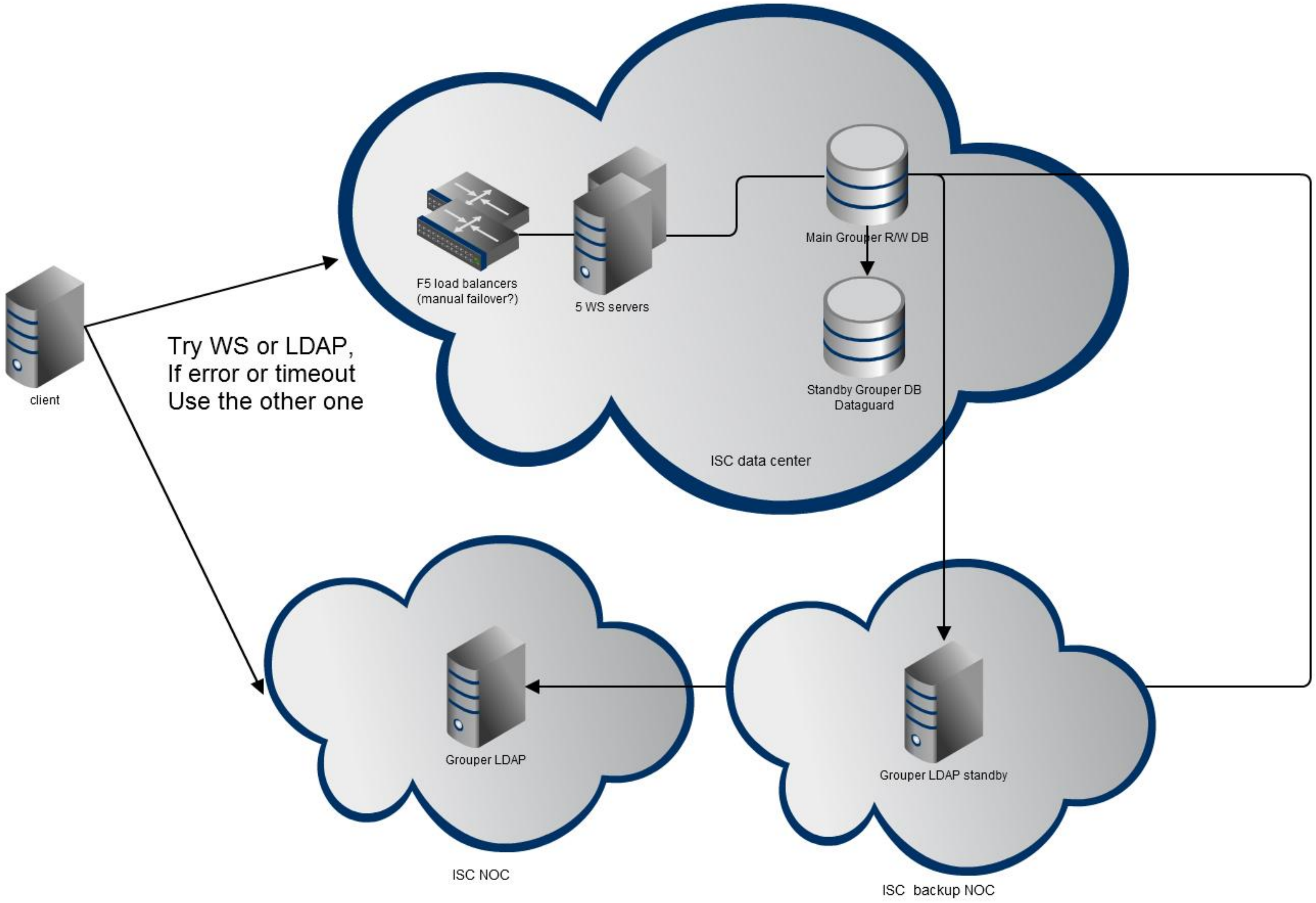
# Previous architecture



# PennGroups access options

- WS
  - Full featured, lots of queries
  - Real time up to date
  - Read/write
- LDAP
  - Updated nightly
  - hasMember and getMembers (not memberOf)
  - Readonly
  - Fast
- SQL
  - Not typical
  - Large exports
- SAML
  - At user login time
  - Only hasMember for groups which are allowed to be sent to SP
  - One hour delay, locally cached in authn system, highly available

# Client failover between WS and LDAP

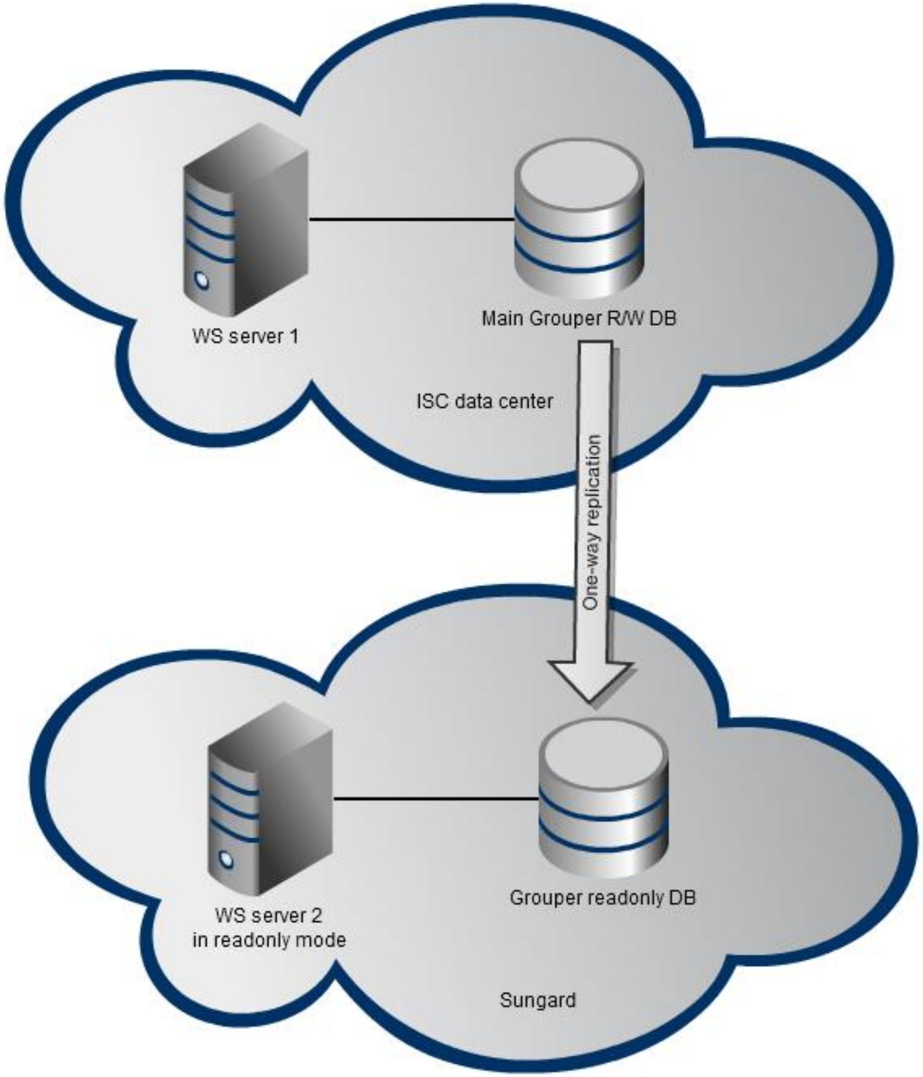


Try WS or LDAP,
If error or timeout
Use the other one

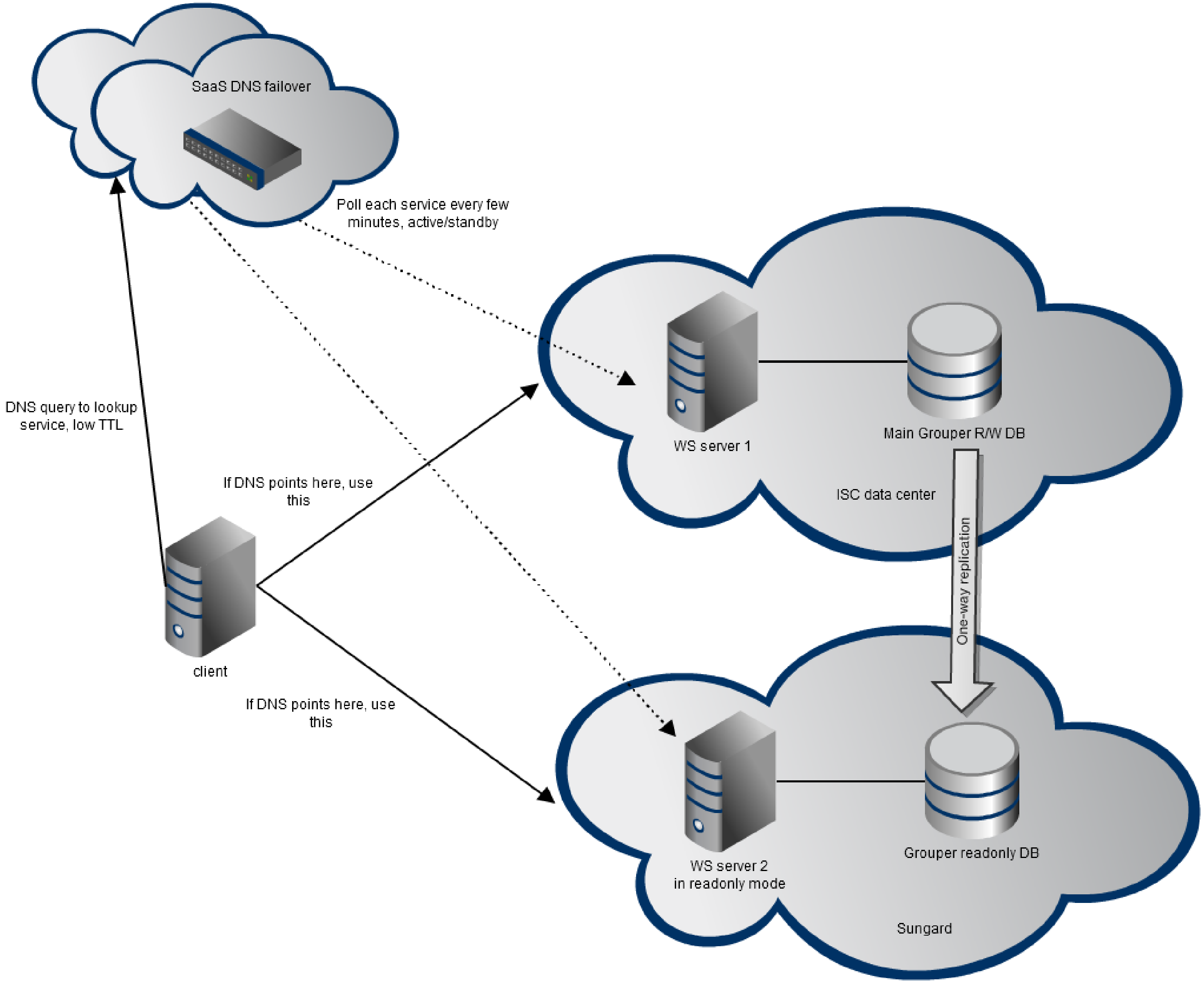
# Client failover between WS and LDAP

- The FAST framework from ISC has done this for years
- Never had an outage
- The logic only does failure failover, not timeouts, need to change that

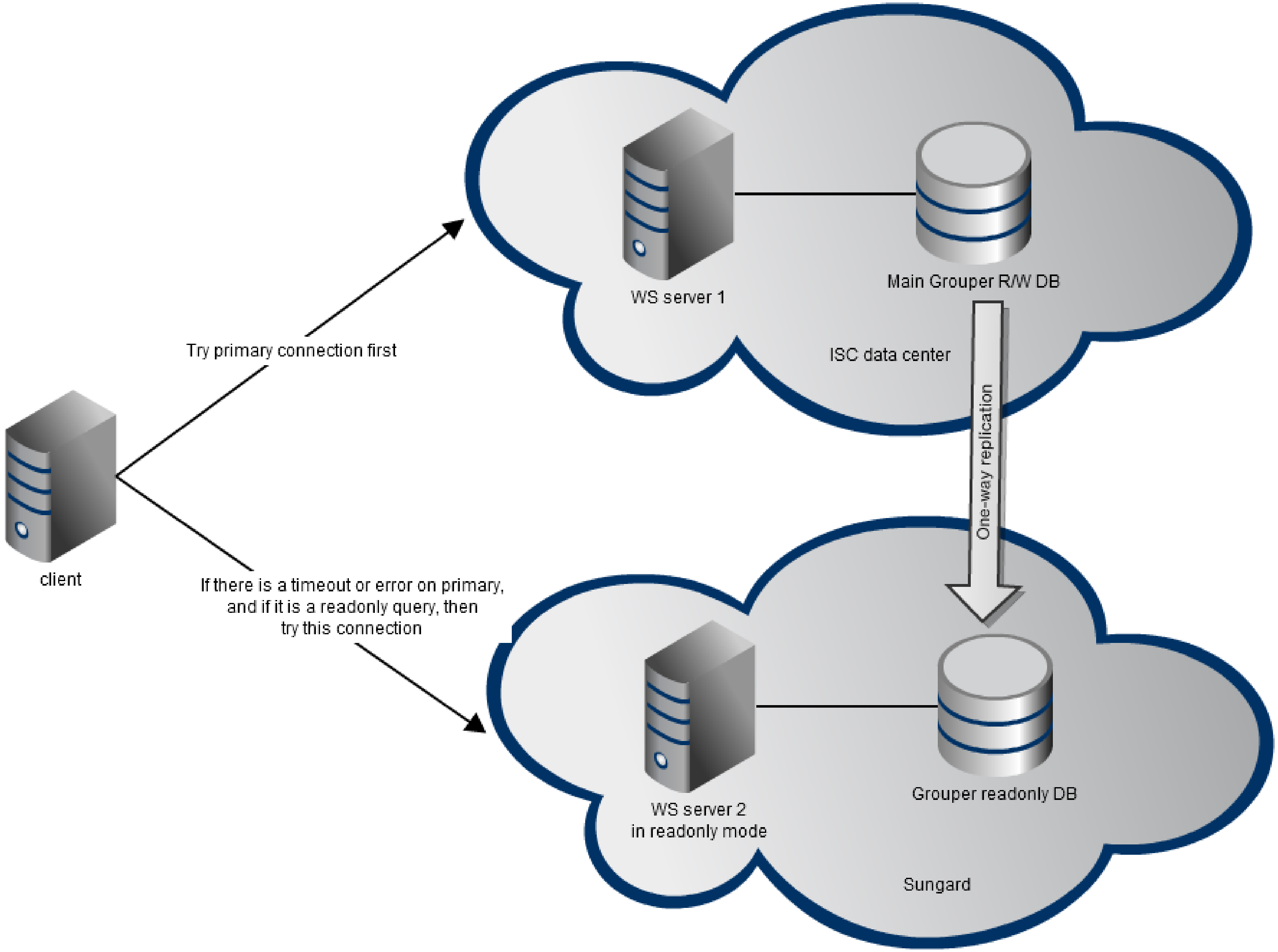
# New read-only offsite WS



# DNS load balancing


SaaS DNS failover
Poll each service every few minutes, active/standby
DNS query to lookup service, low TTL
If DNS points here, use this
client
If DNS points here, use this
WS server 1
Main Grouper R/W DB
ISC data center
One-way replication
WS server 2 in readonly mode
Grouper readonly DB
Sungard

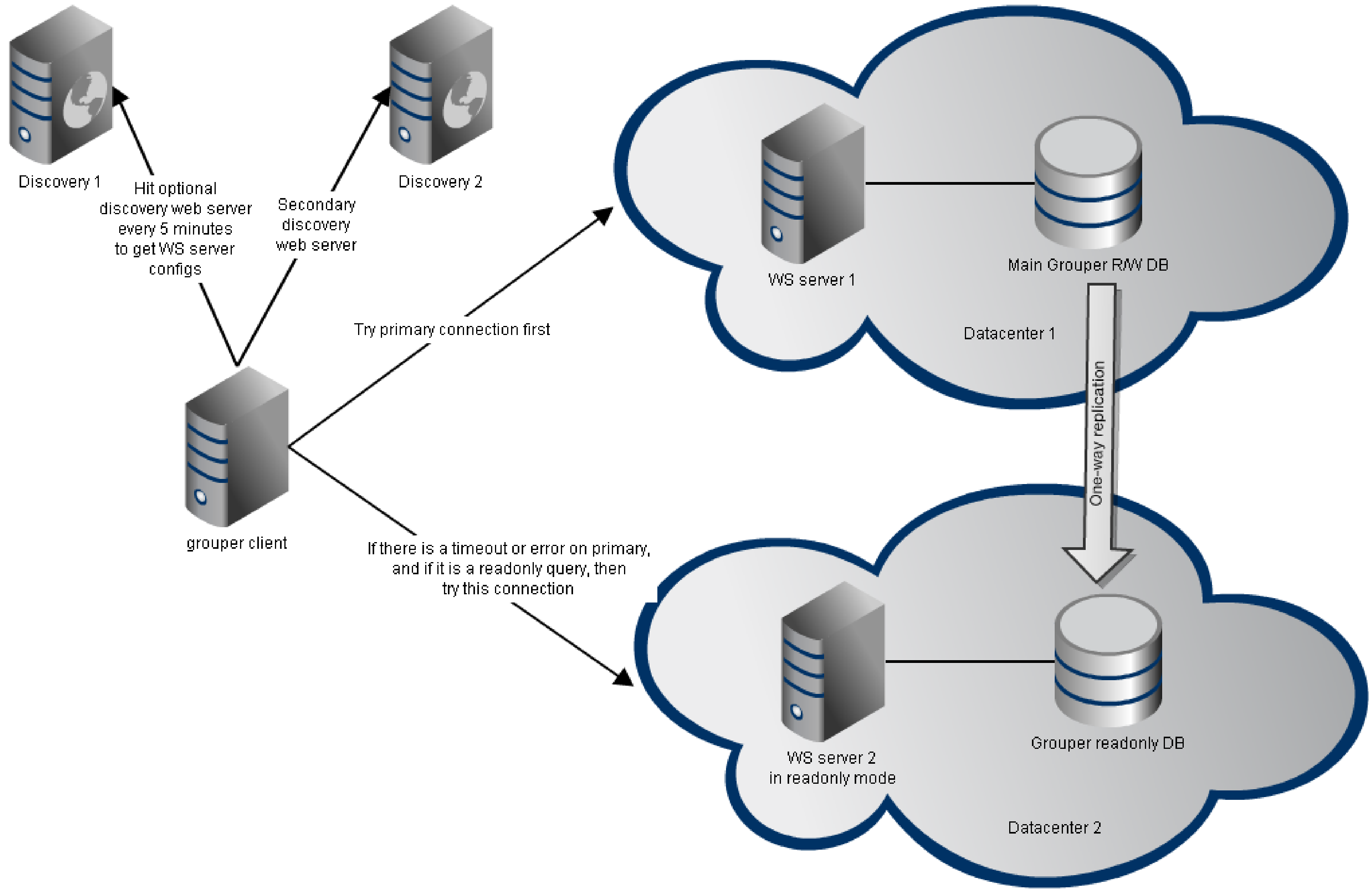
# Client failover between WS's


WS server 1
Main Grouper R/W DB
ISC data center
One-way replication
Try primary connection first
client
If there is a timeout or error on primary, and if it is a readonly query, then try this connection
WS server 2 in readonly mode
Grouper readonly DB
Sungard

# Discovery

- Grouper high available client has discovery
- Allows the service operator to configure which servers are available
- Penn is not currently doing this, but we could

# Discovery



Discovery 1
Hit optional discovery web server every 5 minutes to get WS server configs
Secondary discovery web server
Discovery 2
WS server 1
Main Grouper R/W DB
Datacenter 1
Try primary connection first
One-way replication
grouper client
If there is a timeout or error on primary, and if it is a readonly query, then try this connection
WS server 2 in readonly mode
Grouper readonly DB
Datacenter 2

# Grouper client

- One java jar with no dependencies
- Can be used as library or command line
- Does LDAP and WS
- Failover  between WS on failure or timeout

# Failover comparison

- LDAP or WS
  - Single points of failure, manual fixes might be required for outages
- LDAP/WS failover
  - Only works for LDAP queries, LDAP has daily update and might have stale data, need logic in app
- DNS based failover
  - Few minutes of failover for polling and TTL, secondary server could have stale data though is generally real-time
- Client based failover
  - Readonly queries, need logic in app, 2nd server could have stale data though is generally real-time

# Failover demo

- Try the client for each server in test env
- Try the DNS name
- Turn off primary
- Try DNS, see error
- Try client for each (see one down)
- Try client failover (see warning)
- Try DNS (is it done yet?)

# Failover summary

- Make sure you are on penngroups-users listserv
- Email penngroups-help and let us know you are doing it
- 2nd offsite WS is new, experimental, might change
- DNS load balancing is new, experimental, might change
- Data is generally real-time up to date, but replication could fail for some time

# New PennGroups UI

- Penn uses Grouper 2.1
- Grouper 2.2 will be released soon
- Has a new UI
- Admin and Lite UI still shipped
- New UI does not completely contain all logic in the admin and lite UI (maybe it will in 2.3?)
- Accessible and mobile friendly
- Lot of UX design and studies

# New UI features

- Tree control
- Dashboard
- Favorites
- Recently used
- Services
- Analyze membership
- Bulk assign
- Ajaxy (but bookmarkable and backbutton friendly)

# New UI vs old

- Add group to user
- View/assign privileges
- Deprovision quickly

# Fin

- Thanks
- Email penngroups-help@lists.upenn.edu for info
- This pres will be on the penngroups page (google it)
- http://www.upenn.edu/computing/penngroups/