Delegated Access Control in AD using Grouper

Rob Carter, Duke University
Shilen Patel, Duke University
History
How did it ever come to this?

- **Duke ca. Y2K**
  - Vastly distributed IT
  - Novell, DUMC $$
  - Unix-centric core, MIT Kerberos
  - No IDM
  - Active WHAT?

![Diagram of distributed departments and IT systems](image.png)
How did it ever come to this?

- **Duke ca. Y2K+4**
  - Novell, DUMC $$, growing...
  - *nix-centric core, MIT Kerberos, Novell IDM
  - Mix of AD/NT4/*nix in departments
  - Central AD, largely ignored...
How did it ever come to this?

- **Duke ca. Y2K+8**
  - Novell, DUMC $$, expanded, centralized...
  - Windows/AD + *nix core, late Novell IDM
  - Mix of AD/*nix in departments
  - Limited AD buy-in
2009: The year everything changed

- DUMC $$ fleeing late 2010
- Novell IDM ==> Oracle IDM
- Exchange, ECAL
- Central AD detached but part of IDMS
- Our cheese is up moving around...
Politics, Strategy, and Plans
Conditions (ca. 2009)

- Many (expensive) local AD domains
- Central AD = “privileged resource”
- Central IT: AD = Windows (or worse)
- Community interest piqued by ECAL, Exchange
Politics (ca. 2009)

• Why hasn’t central AD caught on?
  • High barriers to entry
  • Very limited vestment
  • Disconnection = no added value
  • Lack of delivery has led to a trust gap...
Politics (cont’d)

- Solution: Outside-in approach
- Create steering/governance group
- Collect functional requirements
- “Sell” AD more like a service
- ...and then came the six-page manifesto...
Ethel the Frog looks at violence in the British Underworld
The Plan
(They offer to beat us up and let us pay for it)

- Link IDM with AD
- Synchronize K5 + AD passwords
- Load users into one big OU, let admins “sort it out”
- Make departments domain admins -- “trust us”
- Result: Failure to launch
The Plan Fails

- Central IT unwilling to play cop
- Governance indecision - whom to trust?
- Exchange admins, others, want reliable OU map
- So we countered with...
The Other Plan
(Threaten not to beat them up if they don’t pay us)

- Link IDM and AD; sync passwords
- Mirror-image “Departmental” and “People” OUs
- Sync IDM users to People OUs w/ ERP data
- Grant IT staff in departments “Admin” roles, IT managers “Manager” roles
- Asymmetric privileges in “People” and “Depts” scoped to “own” department
- Result: CFIT...
The Other Plan Fails

• Initial “trust” issues resolved, but...
• ERP-based department data unstable; lacks nuance
• All ITers don’t manage AD (OIT = 200 IT staff)
• Inter-departmental IT support agreements
• Security & Audit & Sr. Mgt, oh my!
  • chain of authority; policy; indemnification
• So we tried...
The Other Other Plan
(Threaten to beat them up if they don’t pay us)

- Link IDM with AD; sync K5 passwords; split AD into People and Departmental OUs
- Modify ERP OUs with governed “roll up table”
- Add an “Authority” role and policy sign-off
- No automatic privileging - Authorities to elect ad hoc delegation or delegation to dynamic groups
- This was a turning point...
TECHNOLOGY
Convergence ‘09–’10

- Russ Allberry’s pwsync plugin
- Functional IDM (Oracle)
- SAP-WS orgunit access
- Grouper v1.5+ (with permissions)
- Already 250,000+ groups -- what’s a few thousand more?
First Steps

- pwsync plugin (06/09)
First Steps

- pwsync plugin (06/09)
- OIM integration (10/09)
First Steps

- pwsync plugin (06/09)
- OIM integration (10/09)
- ERP integration (01/10)
First Steps

- pwsync plugin (06/09)
- OIM integration (10/09)
- ERP integration (01/10)
- Depts vs. People (01/10)
First Steps

• pwsync plugin (06/09)
• OIM integration (10/09)
• ERP integration (01/10)
• Depts vs. People (01/10)
• Grouper (v1.5) groups in AD (07/2010)
MODELING
Departmental OUs::Resources

- Map Departmental OUs in AD onto Grouper Resources in One Hierarchy

- OU= DukeDepts
  - Duke:Resources
  - duke:resources:dept_tree
  - duke:resources:dept_tree:TrinityCollege
  - duke:resources:dept_tree:TrinityCollege:DFAS
  - duke:resources:dept_tree:TrinityCollege:DFAS:techsvcs
  - duke:resources:dept_tree:TrinityCollege:A&S
  - duke:resources:dept_tree:TrinityCollege:A&S:Chem
  - duke:resources:dept_tree:TrinityCollege:A&S:Art
  - duke:resources:dept_tree:FinancialServices
  - duke:resources:dept_tree:ChancellorHealthAffairs
People OUs :: Resources

- Map (User OUs x Attributes) onto Grouper Resources in Separate Hierarchy

OU: DukePeople

- Financial Services
  - DFAS
  - tech svcs
  - Users

- Trinity College
  - A&S
    - Chem
    - Art
    - Users
  - Users
  - Users
  - Users
  - Users

 duke:resources:people_tree

duke:resources:people_tree:TrinityCollege

duke:resources:people_tree:TrinityCollege:objectClass

duke:resources:people_tree:TrinityCollege:unixLoginShell

duke:resources:people_tree:TrinityCollege:unixHomeDirectory

duke:resources:people_tree:TrinityCollege:Users

duke:resources:people_tree:TrinityCollege:Users:objectClass

duke:resources:people_tree:TrinityCollege:Users:unixLoginShell


duke:resources:people_tree:TrinityCollege:A&S

e tc...

duke:resources:people_tree:TrinityCollege:Art
Roles::Groups

- Global default cases => dynamic groups
  - managers (employees with management responsibility)
  - it_staff (employees with IT job family)
  - it_nonmanagers (IT-Staff & !managers)
  - it_managers (IT-staff & managers)
Roles::Groups (cont’d)

• Departmental default cases => dynamic groups
  • OU:members (employees in OU)
  • OU:it_staff (OU:members & IT-Staff)
  • OU:it_managers (OU:members & IT-Managers)
  • OU:it_nonmanagers (OU:members & IT-NonManagers)
Roles::Groups (cont’d)

- Explicit groups for the three AD delegate roles
  - OU:adAuthorities (Authority role)
  - OU:adManagers (Manager role)
  - OU:adAdmins (Admin role)
Roles::Groups (cont’d)

- Include/Exclude groups for delegated roles
  - OU:ad_managers_includes
  - OU:ad_managers_excludes
  - OU:ad_admins_includes
  - OU:ad_admins_excludes
Roles::Groups (cont’d)

- Composing groups for the three AD delegate roles
  - OU:AD Authorities (Authority role)
    - Explicitly delegated by OIT
  - OU:AD Managers (Manager role)
    - OU:ad_managers_systemofrecord + OU:ad_managers_includes - OU:ad_managers_excludes
  - OU:AD Admins (Admin role)
    - OU:ad_admins_systemofrecord + OU:ad_admins_includes - OU:ad_admins_excludes
Grouper Permissions::AD

- Map AD Privileges to Grouper Actions
  - ACTION_FULL (full domain admin rights)
  - ACTION_READ (read-only access)
  - ACTION_READWRITE (read/write access)
Grouper Permissions::AD

- Express AD Access Rights as Grouper Perms
- (subject, action, resource)
  - (OIT:SSI AD Admins have full rights in DukeDepts\OIT\SSI [recursively])
  - (OIT:SSI:AD Admins have read-write access to the unixHomeDirectory attribute in DukePeople\OIT\SSI [recursively - ...:SSI:Users:... would be non-recursive])
GLUE
Binding it all together

- Manual & Semi-manual Processes
  - OU “short circuit” table managed manually
  - Script converts table to Grouper resources & seed groups
  - OIT assigns Authorities manually in Grouper
Binding it all together

- IDM-related components
  - IDM reconcilers consume Grouper groups
  - IDM-triggered provisioning routines manage groups in AD
  - IDM provisioner maintains dynamic groups in Grouper
Binding it all together

- Java code consumes Grouper Permissions view every 60 seconds
- Converts Grouper Permissions to AD ACLs
- Maintains State; Computes Diffs
- Read/Modify/Write ntSecurityDescriptor attribute based on ACL changes
SELF-SERVICE
Web UIs

- AUTHORITIES MUST:
  - Accept Policy before doing anything
  - Manage designations of ad_managers
  - Accept responsibility for delegates

- AUTHORITIES MAY:
  - Manage membership in ad_managers & ad_admins groups
  - Assign privileges to ad_admin groups within their OUs
  - View group memberships
Web UIs

- MANAGERS MAY:
  - Manage membership in ad_admins groups
  - Assign privileges to ad_admin groups within their OUs
  - View group memberships

- ADMINS MAY:
  - View group memberships
Lessons Learned

• Governance, Governance, Governance
• Technology is important; Politics is more important
• Functional requirements are sharp at both ends
• Governance, Governance, Governance
Next Steps

• Roll out access to more departments
• Domain migrations and transitive trusts
• Non-windows client support in AD
• Reconciliation of departmental AD groups to Grouper
• Reuse of delegation model (InCommon cert service delegation? Departmental registrars?)
Delegated Access Control in AD using Grouper

Rob Carter, Duke University
Shilen Patel, Duke University