AD Policy Committee
August 19th, 2011
3110 Engineering Building II
3pm-4:30pm

Members: Dan Green, Billy Beaudoin, Joshua Gira, Joey Jenkins, Daniel Henninger, Dan Evans
Guests: Michael Underwood, Debbie Carraway, Alan Gerber

Absent: Tom Farwig, Wes Thibodeaux

Tech Update:
Billy -- needs approval to add the DELTA.CMA.Service account to the “NCSU-Read Memberships” groups so they can have the campus PolyCom CMA service authenticate against AD. No objection from the Committee.

DFS servers -- one more server to go, no news as its proceeding w/o incident.

SCCM Status Update (Billy): held two training courses, tweaking of permissions for dept OUs continues; cron job almost finished. Should go production by end of next week. Will be run hourly. Possible to slice up code to run some perm updates more often couch as collections).

SCCM (Michael): Operating System Deployment. Plan is to provide central groups that would provide self service option to reinstall.
OU\Software Packages\Operating Systems\OU-OS-OS Name-Flavor text-Version

Auto-create Self Service groups: Attach a -SS at the end?

Dan Evans: “At the next Policy Committee meeting, I'd like to discuss automated policing of .admin accounts -- and see if we can come to some basic agreement of how to handle them universally (as well as possibly extending this into any generic, "non-Unity" accounts since nothing enforces the conformity of the recommended .admin naming convention).
We will be meeting within OIT to see how we want to handle some of ours, but I'd like to cover things like password changes, account disabling and deletions (at a minimum) and see if we can all agree and start a process to manage them properly. I hate discovering active, long-gone employees months after the fact. I think we have discussed this in the past, but nothing formal was ever taken away. We may bring some more thought-through ideas to the table with us for discussion.”

monitoring .admin accts

Reporting and Monitoring:

- Disabling .admin accounts associated with KRB_DISABLED unityIDs. No objection from the Committee.
- Current Report needs SAMAccountName instead of CN and expiration time
- Later: All non service accounts should have expiration dates. Annoy for a while and then have them disabled.
- Daily report for stuff not following policy (expiration not set, not following naming convention, expiration > current time + 1 year w/ fudge factor) include upcoming expiration?
- Reports for OU level accounts that don't match naming convention, are disabled, or are inactive
  - need to see how accurate we can be with determining "inactive"
  - Julie Tilley reports that she has many active accounts being reported as inactive
- Fine-Grained Password Policy (FGPP) may be needed to proceed in some cases.

Was determined that further examination of the accounts in question, and discussion via email was required before we could move forward.

[Ran out of time before discussing below -- will handle via email]

NCSU domain policy "Domain-CWDIllegalInDllSearch (KB2264107) Policy"

- causing errors in EventLog: Windows update could not be intalled because of error 2149842967 (Command line ""C:\Windows\system32\wusaexe" C:\Windows\Windows6.1-KB2264107-x86.msu /quiet /norestart")
- Appears to be caused by the fact that the patches in the policy are now being pushed via WSUS and yet we continue to try and push them via this policy.