AD Policy Working Group
August 24th, 2012
3110 Engineering Building II
3pm-4:30pm

Present: **Donna Barrett, Billy Beaudoin, Tom Farwig, Dan Green, Julie Tilley, Daniel Henninger, Joshua Gira**

Absent: Dan Evans
Guests: Derek Ballard, Alan Gerber, Debbie Carraway:

Business handled outside of meetings:

- The following site was approved for addition (and was implemented) to the default Intranet Zone list in IE on client operating systems: Transcripts: https://packtracks.acs.ncsu.edu
- SysNews User Lookup tool -- agreed to add WolfTech domain account information to the SysNews User Lookup tool, including the following attributes:
    - last login time
    - password last set
    - account creation time
    - account disabled
    - lockoutTime
    - CN (cn)
    - Display Name (displayName)
    - Member Of (memberOf)

=====

Agenda:

Add one-way trust from Affiliates -> Wolftech (Billy on behalf of Harry, Connie, Christine)

Purpose -- be the guest account system for parents, VCL, friends of the Library, etc. Separate domain from Wolftech. In order to have Shib or ADFS setup correctly, we need to have a trust setup (Affiliates trusts Wolftech) so all auth would point at the Affiliates domain. Point of contact for the Affiliates domain is Joe Wells or Kevin Swann.

Request: Allow the trust.
Committee: **Approved.**

6th DC for testing of the VM Snapshot/Offsite service (Billy)

Goal is to be able to react to full site network issues by shipping a VM DC off to MCNC (for example) in cases of NCSU-wide issues. The VMware team is currently building a higher load cluster where a DC would more appropriate than the current general use clusters. Once they are done, we'll schedule a time to implement a 6th DC in that environment.

Committee: **No objections.** If possible, do during Fall Break for the least impact on users.

WSUS / Windows8 (Dan)

It would seem that in order for Windows 8 (and probably Windows Server 2012) to be able to get patches from WSUS, that WSUS needs to be running on a Server 2012 server. Unfortunately we host our WSUS service as a VM and Server 2012 requires vSphere 5. -- the NCSU Main clusters aren't currently at that level, but they will be in a month.

So the question is -- can we wait?

Committee: Need to find the MS Windows Update server and set that explicitly for Windows8/ Windows2012 until we have the ability to patch using internal servers.

ACTION ITEM: Update the domain level Windows 8 / Windows Server 2012 policies to use the MS Updates server rather than our default internal server. We're not sure how offsite laptops (SCCM issue) are reacting. Would be good to test this.

More Additions to the IE Trusted Sites (Dan)

Jack Foster has requested that the new SIS and HR systems are added to the windows 7 trusted site list, no later than September, 28, 2012.

cs9prd.acs.ncsu.edu
cs9rpt.acs.ncsu.edu
hc91prd.acs.ncsu.edu
hc91rpt.acs.ncsu.edu

Another requested change: For Trusted Sites, we need to modify the security setting for "Display mixed content" to "Enable" for all sites in the zone. This prevents IE from asking every time SSL encrypted and non-encrypted content is presented on the same page. (Dan's note -- oh heck yes, been meaning to fix this forever as it bugs me constantly in Marketplace!)

Committee: **Approved (both requests).**
ACTION ITEM: Make the GPO changes. Do a secondary post for the SSL stuff. (Billy)

Remedy Service Account (Dan)

We've been asked to permanently add the service account "wolftech\ oit.remedy.service" to the group "wolftech\NCSU-Read Group Memberships".
"I have had a request to modify the Remedy system so as to flag Remedy customers in different ways depending upon their membership in various Wolftech AD groups." Membership in the group is required for his service account to see this.

Committee: **Approved**
ACTION ITEM: (Derek) Please add his account to the group.

Windows 8, SMBv3, and Celerra (Derek)

Basically, Windows 8 wants to use SMBv3 to talk to file servers, but the NCSU Celerra instance won't understand this. We want to create a Windows8 policy that will set its default to use SMBv2 until the Celerra is updated to support SMBv3. Individual units will be able to override this at their level should they have machines where v3 is needed and Celerra support unnecessary.

Technical Details: Tom Farwig posted this link in the AD chatroom recently: http://support.microsoft.com/kb/2686098. From that information, we are implementing one of the workarounds listed in the article. Specifically, setting HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecureNegotiate to a value of "0" (zero) via group policy registry preferences.

ACTION ITEM: Derek is still attempting to get a Group Policy created that will do this. Once he's successful, the Committee says **approved and proceed**. GPO should be limited to Win8/Win2012. GPO must be unenforced to allow local OU admins to override as needed.

NCSU Drive (Dan/Debbie)

The new "NCSU Drive" is public / in production: http://oit.ncsu.edu/unity-accounts/ncsu-drive Need to discuss how we should be reacting at the domain level. Chatroom discussions have revolved around the creation of a domain wide optin group (like how we do software deployments) that would automatically map the "B" drive for users of computers in the optin groups.

Committee: Yes, we should do this. But we want to make sure that we can do it so when you add a computer to the group, the B drive for everyone shows up. No issues with listing as a SW group.

ACTION ITEM: Look at CNR / TSS to see their settings. Need to test for XP, Win7, Win8. Apply at the NCSU OU level. Set the security "read" of the policy to use Unity-users group, not domain users to avoid non-UnityID login errors. Add "NCSU Drive" label. Sysnews post when ready.

Followups/Updates?

- SCCM 2012 (Billy)
  - Test domain setup of SCCM 2007 complete. Working towards installation of SCCM2012 on Test domain. Migration tests come after. Looking like we can retire our 2007 custom delegation code. On track for mid November migration.
- RD Gateway Update (Alan)
  - Server up and working great. Still need docs, otherwise, looking good. TS licenses are still required to use. Announcement "soon-ish".

Action Items Still Pending

- **6/22/12 ACTION ITEM:** Ask Billy to update his "delete all old computer accounts in the NCSU\Unassigned OU" script and add it to the cron server. Also needs to create SysNews post announcing new policy. Add to the activedirectory.ncsu.edu notes.
  - Derek: "Mostly written, still in testing". Should be able to go live in next couple weeks.
- **6/22/12 ACTION ITEM:** Create a document to outline a process to follow in this situation (WTMG group management for immediate termination). (Dan G)
- **4/27/12 ACTION ITEM**: Alan/Joe coordinate w/ Derek to get the new RDS-G server into the appropriate OU / security group. Once service is up, document on AD website.
  - see above

- **4/27/12 ACTION ITEM**: People intrigued and agree that shaving 30secs is a good thing -- Billy, go figure out details of using shadow groups for OS's to defer WMI query times.
    - After further investigation, will create and fill the shadow groups, but only want to update the domain level SERVER (not workstation) policies. Timing issue could cause workstations to not correctly see their security settings until its rebooted a time or two. While also true for servers , less of an impact as admins interact much more during the setup of the server. Research done; no code yet.
- **12/16/11 ACTION ITEM**: create a domain wide (optin) GPO for enabling Bitlocker for domained machines; schedule this subgroup to get together and flesh out.
    - REALLY NEED TO TAKE CARE OF THIS.

Announcements:

- Debbie hired new AD Architect position.
- Billy wants to make changes to how we're dealing with AFS clients and the loopback adapter. He'll provide more information for discussion via the list.