AD Policy Working Group
June 22th, 2012
3110 Engineering Building II
3pm-4:30pm

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

Guests: Michael Underwood, Derek Ballard

Business handled outside of meetings:

- Removed all computer objects in Unassigned OU with create/mod dates pre-2012.

=====

Agenda:

“uninstall when falls out of scope" and Security-based forced upgrades (Billy)

Despite Dan's efforts to harass people into upgrading their software, we've still got alot of the old Firefox, Quicktime, Java, Flash, etc packages being used. A couple folks I've talked to seemed worried about dropping their group memberships because of worries about forced uninstalls of newer versions that had been installed over top of the old one.

I'd like to propose that for some of the ancient software packages we

- disable the "uninstall when falls out of scope" option on ancient software packages
- and possibly drop the computers into a newer package.

Note that I am only talking about things that are security issues (browsers, browser plugins, etc) and those that are no longer getting security updates (like the ~3000 computers with Firefox 2.x or 3.x).

The following is what this might comprise (pulled together by Dan Green) plus usage numbers:

- FW-Adobe-Acrobat Reader-8.0-20070307 (51)
- FW-Adobe-Acrobat Reader-9.1-20090417 (22)
- EX-Adobe-Acrobat Reader-9.1.3-20090727 (23)
- FW-Adobe-Acrobat Reader-9.2.0-20091015 (69)
- FW-Adobe-Acrobat Reader-9.3.3 (44)
- EX-Adobe-Acrobat Reader-9.3.4 (175)
- FW-Adobe-Acrobat Reader-9.4.0 (1290)
- EX-Adobe-Acrobat Reader-9.4.1 (7)
- FW-Adobe-Acrobat Reader-9.4.2 (739)

- FW-Adobe-Flash Player-10.0.22.87-20090506 (36)
- FW-Adobe-Flash Player-10.0.32.18-20090810 (89)
- FW-Adobe-Flash Player-10.1.102.64 (1946)
- FW-Adobe-Flash Player-10.1.53.64 (387)
- FW-Adobe-Flash Player-10.2.153.1 (531)
- FW-Adobe-Flash Player-9.0.45.0-20070619 (54)

- FW-Adobe-Shockwave Player-10.1.4.020-20061024 (3)
- FW-Adobe-Shockwave Player-11.5.1.601-20090810 (88)
- FW-Adobe-Shockwave Player-11.5.10.620 (744)
- FW-Adobe-Shockwave Player-11.5.7.609 (62)
- EX-Adobe-Shockwave Player-11.5.8.612 (1)
- FW-Adobe-Shockwave Player-11.5.9.615 (2566)

- FW-Apple-QuickTime Player-7.1.5-20070307 (182)
- FW-Apple-QuickTime Player-7.5.0-20080611 (46)
- FW-Apple-QuickTime Player-7.62.14-20090728 (1861)
- EX-Apple-Quicktime Player-7.66.71.0 (27)
- FW-Apple-Quicktime Player-7.69.80.9 (1568)

- FW-Google-Chrome-10.0.648.204 (936)
- FW-Google-Chrome-6.1 (267)
- FW-Google-Google Earth-5.1-20091209 (364)

- FW-Mozilla-Firefox-2.0.0.4-20070531 (198)
- EX-Mozilla-Firefox-3.5.1.0-20090727 (22)
- FW-Mozilla-Firefox-3.5.2.0-20090810 (77)
- FW-Mozilla-Firefox-3.6.0-20100303 (12)
- FW-Mozilla-Firefox-3.6.12 (1372)
- EX-Mozilla-Firefox-3.6.15 (2)
- FW-Mozilla-Firefox-3.6.16 (877)
- EX-Mozilla-Firefox-3.6.17 (486)
- FW-Mozilla-Firefox-3.6.3-20100412 (78)
- FW-Mozilla-Firefox-3.6.8 (404)
- EX-Mozilla-Firefox-4.0.0 (29)
- EX-Mozilla-Firefox-4.0.1 (144)

- **SW-Real-RealPlayer Ent-6.0.11.2160-20090728 (1395)**
- FW-Real-RealPlayer-10.5-20050929 (2369)

- EX-Oracle-Java JRE-1.6.24 (527)
- FW-Sun-Java JDK-1.6.20 (6)
- FW-Sun-Java JDK-6.0 u14-20090803 (24)
- FW-Sun-Java JRE-1.6-20080812 (3)
- FW-Sun-Java JRE-1.6.20 (198)
- FW-Sun-Java JRE-6.0 u13-20090723 (1291)

- FW-VideoLAN-VLC Media Player-0.8.6f-20080507 (2196)

If we wanted to sort out the following, we'd need to provide a newer Acrobat Pro 9.x package (9.5.1 is the current patch version) as they'd not necessarily be licensed for 10.x.

- SW-Adobe-Acrobat Professional-9.1.0-20090423 (1)
- SW-Adobe-Acrobat Professional-9.2.0-20091014 (10)
- SW-Adobe-Acrobat Professional-9.3.2 (746)
- SW-Adobe-Acrobat Professional-9.3.4 (10)
- SW-Adobe-Acrobat Professional-9.4.0 (404)
- EX-Adobe-Acrobat Professional-9.4.1 (47)

- SW-Adobe-Acrobat Professional-9.4.2 (271) -- don't delete this one on Labor Day unless Tom has created a newer version.

Thoughts / Discussion?
Removing the Uninstall / Scope part sounds great. Plan for July 1st implementation?
Deleting the groups in a month -- how about waiting until after Labor Day? September 4th. Gives groups more time to move themselves to newer groups. We may need to look more carefully at the bolded packages. Committee does not want to force move the computers in these software groups to a newer group -- two months should be enough time for those who wish to move their computer objects themselves.

ACTION ITEM: Send out Sysnews/AD list post that explains all of this, then do as scheduled. (Dan G)

New Policy: Delete all old computer accounts in the NCSU\Unassigned OU (Dan Green)

I'd like to propose that we enact a policy w/ associated script to clear out any computer accounts in the NCSU\Unassigned OU where the following 4 attributes are all older than 6 months:

- whenCreated
- whenChanged
- lastLogonTimestamp
- pwdLastSet

Earlier this month we cleaned out anything that was pre-2012, deleting approximately 3/4 of the accounts in that OU. I'd like to automate this process. Any of them that meet those pre-reqs haven't talked to the domain in any way in 6 months, and because of the GPO's set, no one should have been able to log into them in that state. So we believe people just haven't cleaned up after themselves.

Thoughts / Discussion? Committee says do it.

ACTION ITEM: Ask Billy to update his script and add it to the cron server. Also needs to create SysNews post announcing new policy. Add to the activedirectory.ncsu.edu notes.

Domain GP Update: Trusted Intranet Zone and ComTech VPN

- there was a discussion of the ComTech VPN client and adding additional objects to the intranet zone in the domain client OS policy to make the installation go smoother.
- Specifically, dc1-vpn-1.ncstate.net, dc1-vpn-2.ncstate.net, dc2-vpn-1.ncstate.net, and dc2-vpn-2.ncstate.net

Discussion, Recommendations, Objections? No objections.

ACTION ITEM: Update WolfTech-Default Domain Policy - Desktop OS policy and announce change to SysNews. (Derek)

WTMG group management for immediate termination (Dan E.)

We get requests from our supported departments to remove users due to termination. Sometimes these are in the form of "We are headed into the meeting now. Can you terminate userX's access to the department's computers and network shares in the next fifteen minutes?"

Relying on WTMG groups to grant access, this is virtually impossible without tracking down a domain admin to remove the user from the group, which will re-populate on the next build unless PeopleSoft is updated. Simply disabling the account might be problematic if user also a student.

How are other groups working through these requests and managing "exclusions" to WTMG's?

Not truly an AD issue, but tied to WolfTech's Identity Management and "WTMG" applications... (while the latter is tied directly to AD, the former feeds many applications). Dan G is going to work with Dan E on a shortterm solution, and then think about if we should be working at an update to WTMG to allow exceptions at that level, or if it should be done at the top level of WolfTech's Identity Management system -- aka, affecting not just Active Directory groups, but also webpage access controlled via GuardDog, list memberships maintained by ListMinder, etc.

ACTION ITEM: If nothing else, we *do* need a document to outline a process to follow in this situation. (Dan G)

Michael's SUP patching

(There's been some confusion; I think some explanations, discussion in the committee could help. Michael agreed to come and help fill in the blanks with regard to patching via SCCM.)

SUP groups are used for software updates via SCCM. Why? "Better reporting of patches" was given, but the committee questioned this. There was later questioning of why we aren't using the SCCM WSUS server fully for OS patches and SCCM SCUP for non-OS patches.

SUP -- we have early, normal, late collections in SCCM based on the keys (key set by the WSUS Target Group that OU Admins set in their group policies) inventoried by the SCCM client:

- SUP-WSUS-Early (Patch Tues)
- SUP-WSUS-Normal (Patch Thurs)
- SUP-WSUS-Late (Patch Next Tues)

(mirrors the timing of the current WSUS groups with the exception of Early which currently get patches as they're released rather than waiting until Patch Tuesday)

Michael uses these collections to assign patches via SCCM. Patches installed at 3am on the computers. No rebooting (and this cannot be changed by individual OU Admins), but endusers do get notification that you need to. Auto-approve rule exists for all "definition updates" to autodeploy immediately (though this is being done via the SCCM WSUS server, not SCCM).

NCSU-EX-Microsoft-SUP-AUTO -- security group that people can use to point at the SCCM WSUS server.

- 60 odd computers in -SUP group, yet 1000+ machines pointed to new server.
    - why the discrepancy? software update client part of SCCM client has been triggered/activated. This changes the WSUS server on the local client (any machine with the SCCM client installed). During the next Group Policy refresh, it sees the correct (original server) and fixes it. If you're off campus, your computer

can't talk to the GP policy and so it remains talking to the SCCM WSUS server. These computers (mostly laptops) + the EOS labs + the EX-SUP-AUTO group members should account for the computers that are talking to the SCCM WSUS
- 7960 unapproved patches on the SCCM WSUS server?
    - These are being downloaded into SCCM. WSUS will lie to you. The only correct information / reporting would now be in SCCM.
    - https://oit100sccm-rp.oit.ncsu.edu/reports -- login with wolftech\unityid.admin

Acrobat-AUTO is the only current SW group that requires you be in the NCSU-EX-Microsoft-SUP-AUTO group as well if you want it to remain patched. Chrome-AUTO and Firefox-AUTO software groups do not require this.

Followups/Updates?

- Followup on WolfAlert to the Desktop (Dan)
    - Seems to be two different groups (Fire Marshall and WolfAlert) looking for a way to send alerts to the desktop -- and they're contacting different groups hoping to get emergency notifications made available.
- SCCM 2012 Update (Michael)
    - WolfTest is fully rebuilt. Waiting on meetings to be scheduled by Gene Morse. SP1 already announced at TechEd. Michael still hopes to have a production environment by Winter Break.
- Secunia / Shavlik purchase didn't happen, funding gone. No other information was available.

New Business

- Derek has been asked to help add the AD info to the User Lookup tool in SysNews. Committee agrees that this would be good, though would like to know what information will be displayed BEFORE it goes live.
    - **ACTION ITEM:** Derek, please followup with a list of attributes that will be shown on the Sysnews User Lookup page.

For the Record...

Services Now Authenticating Against WolfTech AD:

- Campus Voicemail
- New WolfPrint (Papercut)
- Remedy
- KBox
- VMware
- Mediasite
- Casper
- Citrix
- Urchin