AD Policy Working Group
June 21, 2013
3110 Engineering Building II
3pm-4:30pm

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

Guests: Alan Gerber

Business handled outside of meetings:

- Nothing to report.

=====

Agenda:

WDS Service Changes (Alan Gerber)
Summary from Alan of the recent boot image changes in WDS and upcoming XP end of life within the WDS service -- why they're necessary and what they'll mean for campus.

Changed to Windows 8 boot image as default.
Added multiple drivers from numerous requests.
Different driver support based on OS. Less OSes help reduce service complexity.

No complaints have been sent to Alan; no one has registered any objections to the obsolescence of Windows XP images. There has been no noticeable usage of the XP base image in many months (image is also last updated in 2010; rather out of date). Only custom images were/are from OIT, CHASS, and CVM -- all of which are OK with this -- all have also gotten little usage this year.

It *is* still possible to submit a custom XP image should something come up.

Moving forward driver updates should be a group effort. Training materials are being generated that will walk folks through it; possibly as earlier as the end of the month. Also mounting / removing custom images.

SCCM driver repository -- it is a separate task from WDS driver management.

Debbie has volunteered one of her staff to assist. Richard Norris/Dustin Duckwall from CNR and possibly someone from OIT Managed Desktop Tech Team as well (to be determined).

Billy -- “ok, so who’s the backup for when something goes wrong and we need someone to diagnose a problem with the system.” We still need to address the issue of high level backup support for Alan. One of the benefits of bringing in lesser tech for the day to day is that perhaps he’ll have more time on the big stuff. Though if Alan’s on vacation, we’re in trouble.

Dan E -- we need to make it a part of the administrative process that anytime you add a driver to the system you’re either noting it in the Remedy request OR if you’re being preemptive, CREATE a remedy request to log.

ACTION ITEM (Alan): there is a way to manually install an image via USB when you can’t wait for the WDS service to be updated. Please add this to the AD doc website.

Service Group Changes (Dan)
10/26/12 -- discussed adding Derek to assist Alan with WDS, and was noted that Gene Morse was also interested. See above for discussion.

Derek Ballard (one of the domain admins) will be split 50/50 with ITECS and OIT for the next year.

There is also plans to beef up the SCCM / WSUS groups (see below).

Packaging Update
Dan Evans / TSS had previously offered to package all apps that go through Coker for licensing. Wanted to see if there were any updates on this.

- 1st interview this morning. Plan to make an offer soon. Probably won’t have anyone in time for much packaging for this fall’s requirements, but want to move into a packaging service for campus in the near future.
- Expectation/hope is for the OIT Managed Desktop tech team to also pick up some of the level 2.5 support for AD, SCCM and possible WDS to alleviate pressures on volunteers as much as possible.

There is a meeting next week to try and get Secunia up and running before the start of the Fall. In addition to vendor drivers (think Dell), this will address the need to update Firefox, JRE, JDK, Flash, Shockwave, Acrobat Reader (updates but not initial install), Acrobat Pro (updates but not initial install), Chrome, Quicktime, Itunes, Pid0gin, VLC, WinSCP.

LDRPS and IE10 (Dan)
“Previous releases of .Net Framework have the EnableIEHosting setting enabled, but Microsoft has disabled this setting in .Net Framework 4.5, which prevents applications from working that

require this setting to be in place. Specifically LDRPS 10 requires this and now no longer works with computers that have been upgraded to .Net Framework 4.5. Is this a good candidate to be rolled out by GPO at the domain level?“

Both Billy and I have stated that this is a bad idea (the IEHosting feature is a vulnerability that was closed for a reason) as a domain wide policy. A software group could be created to edit the registry to turn it on and only those workstations of the folks that need LDRPS can be added to it. Wanted to mention it to this committee and gather input in case a formal request is made.

Billy brings up the idea that for examples like this (also singularity requiring specific version of java, there are more) that we’re now licensed to purchase AppV on campus and this could be a way to tackle this. Better than trying to keep the entire machine on older versions.

Billy -- time to create another OU for random stuff that we’re dropping into SW groups, but aren’t. “Special Configurations” unit-SC-blah for the naming convention.

ACTION ITEM: Create the groups above; edit the automated scripts; and announce to the world.

Technical Update (Billy):
Fine Grain Password Policies -- we’ve previously discussed the need to enable these. Will allow for us to have password policies based on security groups (aka, OU Admins have one; regular Unity accounts follow another).

Groups to initially define for FGPPs:

- Domain Admin -- CENSORED[redacted]y.
- UnityID -- will match what we have now with no reset/expiration dates.
- OU Admins (based on membership in the “NCSU-Departmental OU Admins” group hierarchy, not based purely on the .admin extension) - minimum of 16 chars; lockout at 10, same duration; turning on the complexity (uppercase, lowercase, special char); passwd change interval once a year; pwd change history: 2.
- Service Accounts / Others -- will match what we have now with no reset/expiration dates.

The technical folks with be defining the policies for each of these groups (passwd complexity, duration, history, lockout policies, etc). UnityID policy will match the current domain passwd policy -- everything else will be updated.

Once in place, if there were groups on campus who wished to request additional policies to cover special accounts of their own.

ACTION ITEM (Billy): Date will be picked and announced out to the community, and FGPP enabled. **Committee Approves.**

Old Topics

- 4/19/13 ACTION ITEM: Application Evaluation Deployment cycle (if deployment fails, retry at this interval) -- currently it runs once a week. We think it would be better to run it once a day. (Billy) --- **COMPLETED**.
- 4/19/13 ACTION ITEM: ADMX additions/updates of Frontmotion Firefox, Chrome, and Office 2013. If we can edit the ADMX to specify that its FrontMotion Firefox, we should do so, and explain in Sysnews post. (Derek) -- **Office done / Chrome done / Derek's still looking at the edits we requested of the Frontmotion Firefox.**
- 4/19/13 ACTION ITEM: We need to put out a public request for additional backups from the community. We also need to formally write up a needs assessment -- showing shortcomings and pass the resources request up through the governance committees. -- **Handled via alternative means (see minutes above).**
- 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.
    - **Billy: Will follow up.**
- 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)
    - **No change.** Dan feels bad about this. The other Dan is considering abandoning WTMG for complex groups... may have found a workaround by using a file-system DENY group to remove rights to a share for a particular user whenever necessary.
- 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.
    - Derek: Should be able to go live in next couple weeks.
    - **Alan: It's there and working, but we've never announced. There were still licensing issues (as in, you have to buy some). We just need to toss up a page about the service. We need to check the most recent licensing that Bill Coker has negotiated (including the VCL licenses) to see if this has changed.**

Microsoft License Changes (Billy)

Had license for Windows Server, SCCM server/client, and ….
Microsoft decided to kill these off and we're now running the Windows Core CAL instead. This gains us ForeFront Protection, SharePoint, Exchange, and Systems Center. And we're now able to license the MDOP software that would provide us AppV, AGMP, and other stuff.