AD Policy Working Group
December 13th, 2013
3110 Engineering Building II
3pm-4:30pm

Voting Members: Donna Barrett, ~~Charles Cline~~, Dan Green, Julie Tilley, ~~Dan Evans~~, Daniel Henninger, ~~Tom Farwig~~, Joshua Gira

Ex Officio Members: Alan Gerber, ~~Michael Underwood, Gene Morse~~

Guests: Emily Lynema, Billy Beaudoin

Business handled outside of meetings:

- **Added SCCM Service Team Leads to the AD Policy mailing list (10/21/13)**
  As a part of the creation of the SCCM Service teams I'm going to be proposing that we add the leads of each group to the AD Policy mailing list (and google docs). While they won't have a vote, they will need to be able to participate in the email discussions and offer feedback just as they would at the physical meetings. While we're still getting the service teams sorted out, I've gone ahead and added Alan Gerber and Michael (two of the proposed leads) so we can continue discussing the SCCM / Powershell issues we had on the last agenda.

  Updated 11/08/13 -- added Gene Morse, proposed lead for SCCM Core Service Team.

- **SCCM Client PowerShell Execution (10/23/13)**
  Alan Gerber reported that the CU3 update to SCCM did not resolve this issue (discussed in detail in our last agenda). Committee was asked to decide between approving the change to the client settings to allow unsigned scripts to run, or alternatively make the policy decision that Powershell detection scripts will not be supported in our SCCM implementation until Microsoft fixes its handling of script data. **ACTION:** ***Committee Approved and asked Alan/Michael to implement / announce the change.***

- **AD Policy Committee Membership (11/07/13)**
  Dan Green presented request to move the OIT Security seat from the AD Technical Committee to the AD Policy Committee to the ITSAC-CAS committee. ITSAC-CAS Unanimously Approved; Dan updated AD governance website/mailing list. Tim, the current rep has announced he's leaving NCSU, however, so a new rep will need to fill the slot. Additionally, Billy has been replaced as the Chair of the AD Tech Committee by Charles Cline who will now be a voting member of this committee per our charter.

- **IE11 ADMX Added to Central Store in Domain (11/08/13)**

Dan Green requested that we add the newly released Internet Explorer 11 ADMX files -- http://www.microsoft.com/en-us/download/details.aspx?id=40905&WT.mc_id=rss_alldownloads_all -- to the WolfTech domain central store. **ACTION:** ***Committee: Approves and instructs Domain Admins to install and announce.***

- **Increase SCCM software update timer change request (11/12/13)**
  Billy Beaudoin proposed changing the randomization timer for SCCM patch installation from 2 to 4 hours. Some of the outages lately with networking and san issues are being caused by things getting hit too hard because no one is really using maintenance windows and accepting default settings.

  We'll use script (http://gallery.technet.microsoft.com/scriptcenter/How-to-Disable-the-c3b29b29) to increase the setting to 240.

  ACTION: Committee Approved and was implemented by Domain Administrators (see https://sysnews.ncsu.edu/news/5282419b for details).

- **Throttling SCCM downloads to VM's (11/12/13)**
  Billy Beaudoin added that In addition to pounding the SAN at patch install time, the VMware servers are also pounding the system when patches become available for download.

  "Currently it doesn't look like there is an accessible timer to control that. Also, I don't think creating a bunch of separate deployments to stagger them is a good idea. So instead I'd like to propose creating a collection based on the MAC address prefix assigned by OIT's VCenter (00:50:56:89) and assigning a Client Settings package that turns on BITS throttling (which is currently off). If throttling is turned on, the highest it can be set to is 9999Kb, which is not terribly high (so it would quite effectively throttle the downloads and stop the slamming. But for just downloads by the SCCM client from the SCCM DP's and only for VM's in OIT's VMware infrastructure, this will probably be sufficient."

  Note: The only concern really is that it would also slow down self service app downloads.

  ACTION: Committee Approved and was implemented by Domain Administrators (see https://sysnews.ncsu.edu/news/5282419b for details).

- **Windows 8.1 ADMX files in Central Store (11/27/13)**
  Proposal by Dan Green: Add Windows 8.1 / Server 2012 R2 ADMX files to the Central Store in WolfTech. As with all ADMX file additions, no negative impact is expected (just let's us set policies for these machines), and initial testing of the import has been successful on the WolfTest domain.

  ACTION: Committee Approves and Requests the Domain Admins announce via

SysNews and update the domain.

=====

Agenda:

App-V 5.0/UE-V 2.0 ADMX files import to Central Store

- Proposal by Alan Gerber: Add App-V 5.0 & UE-V 2.0 ADMX files to the Central Store in WolfTech. MDOP 2013 R2, which was just released, comes with new versions of - and thus new ADMX templates for - the App-V and UE-V clients. Details & download link.

ACTION: Committee Approves and Requests Domain Admins to add new ADMX files to the central store.

Patching Schedule for Normal & Late Groups (Dan G)
VMWare Infrastructure folks have noted a strain on their services during the monthly patch releases. They're able to see when all of the campus machines begin to download patches for installation via SCCM. And its taking a toll. They're especially worried as more machines are patched via SCCM rather than WSUS and how that scale increase might negatively impact other services

While we have spread the impact of the installations/reboots, we don't have the option to easily spread out when machines begin downloading -- they will all immediately begin based on the schedule we've established.

Policy Committee does not think that there would be any major issues with moving the release of the scheduled SCCM patches from the current time of 8am to 5pm -- moving the impact of machines / VMs downloading patches outside of the daytime hours and helping to reduce the load on the VM infrastructure.

Most machines aren't being scheduled to install the patches or reboot until early the next morning (3am is the default) so downloading the patches at 8am is much earlier than needed. Notification should be sent out to campus for those who have selected to patch earlier than the default so they can either adjust their schedule or explain the issues this change would have for them.

Emergency patches can still be set with an immediate deadline, so they're not affected.

Another option would be to move it from 8am to even earlier 4am, 5am, for example. There was some concern with overnight database processes being affected… but this would allow a larger window for folks who want to patch during the day and not have their machine reboot in the

middle of the night (aka, researchers).

Neither of these really solves the issue -- just moves it to a time that has less of an impact. The only true way to spread the download time would be the creation of multiple deployment groups throughout the day. Each would have the same deadline, and general settings, but one would start at 8am, another at 9am, and so forth… we would then have to script something to distribute machines in the Normal group evenly among these deployment schedules. Doable and much more scalable, but requires scripting that we don't yet have much of.

ACTION: Talk to Patching Service group to see what they think about moving the initial download from 8am to 5pm on the Normal/Late days. Early groups not applicable. Service team assesses during the January patch cycle to see if it helps alleviate some of the issues -- or at least buys time as more and more devices take advantage of the service. Investigation of the other options should also occur.

Office365 Licensing / Implementation discussion (Billy / Dan G)
Campus is investigating licensing of the Office365 service for students across campus. ADFS will be required to provide the student account information to Microsoft. What infrastructure do we have for this? Who will be responsible for implementing? License will cover virtualized environments -- aka, we can put Office back on VCL images.

Campus Wide Microsoft Dreamspark discussion (Josh Gira)
Bill Coker has asked Microsoft if it would be possible to have a campus wide membership of DreamSpark Premium, associated with STEM classes. Currently, each college is responsible for maintaining their own membership.

Procedure for Units to Request Read to Attributes in AD Groups/Accounts (Billy)
Specific request: Libraries wants access to the ncsuCampusId attribute for user accounts in the People OU. This is now possible to delegate within the normal UI in ADUC. Would like to create a group similar to how we manage the NCSU-Read Group Memberships group. Software will be locally hosted by Libraries (will allow student card swipes to populate unityID into reservation system).

Request: Create new security group that would allow access to this specific attribute on user accounts within the People OU. RSAT tools now allow this to be set without major technical difficulties. Once group created, we'll initially add the LIB.journey.service account provided by Libraries.

ACTION: Committee Approves and Requests that Domain Admins implement. (completed 12/13 by Billy)

Security Representative
ACTION: Remember to invite S&C rep now that Tim has left NCSU. (completed 12/13 by Dan

G)