**AD Policy Working Group**
**June 20th, 2014**
**3110 Engineering Building II**
**3pm-4:30pm**

Voting Members: Donna Barrett, Charles Cline, Dan Green, Julie Tilley, Michael Underwood (proxying for Dan Evans), ~~Daniel Henninger~~, Tom Farwig, Joshua Gira, Payman Damghani

Ex Officio Members: Michael Underwood, Gene Morse, ~~Jonn Perry~~

Guests: Billy Beaudoin

---

**Business handled outside of meetings:**

- **Remove the "NotifyOnly" Client Health Remediation [Billy B.] 5/19/14**
  We set a setting for the SCCM client to not auto-fix issues (like WMI corruption) because the Windows Management Framework 3.0 freaked out the SCCM 2012 client we initially roled out. I think it would be a good idea for us to pull that setting and let the client fix the machine. WMI corruption was pointed out as one of the issues with doing Trend->Kaspersky upgrades.
  **ACTION:** Committee Approved 5/19/14 and Requests AD Tech Comm Review then pass to SCCM Service Team for implementation.

  UPDATE: leave the “on” setting in place until July 15th, then remove policy reference.

- **Force Migration to Kaspersky AV June 11th [Dan G] 5/26/14**
  At the AD Tech Comm on Friday, the committee discussed the need to force the deployment of the Kaspersky AV client (and removal of the Trend client) across the domain computers.

  The Trend license expires on June 28th.
  The AD Tech Comm decided to implement the push on June 11th at 8pm.

  It's important that we announce this date out to the OU Admins as soon as possible as many will want to start scheduling their upgrades ahead of this date or will want to let their endusers know of the upcoming upgrade.

  The Kaspersky install has been altered to now provide all client side alerts (we normally turn this off) when its been installed and if it requires (it does) a reboot from the enduser.

Something to note -- when the software is installed on a computer, a reboot is required before its functional. Scheduling it late on the 11th, means that it will install just ahead of June's patches -- far enough that there shouldn't be any conflicts with those patches that'll get released to "normal" groups the next morning, and yet close enough to take advantage of the reboot associated with the patch deployment. It's still preferable to reboot immediately after installing the client, but for those folks who would ignore this, at least they'll have a patch related reboot in the 24-48hrs following. It's not perfect, but for those that wait for the forced upgrade, at least its something.

I know that this doesn't give us much time. I know that the management consoles haven't yet been provided to us. But we're staring at a drop dead date for Trend that's fast approaching and this seemed the best compromise.

**ACTION:** Committee Approved 5/28/14. Announcement needs to be made to AD Community.

- **SCCM Update to 2012R2 CU1 [Dan G] 5/29/14**
  The SCCM service team is readying to upgrade the SCCM service to 2012R2 CU1.

  The first step is an upgrade of the site server that will take place on June 2nd. There will be no/minor impact on the SCCM service and it will not require any updates on the client workstations. As such, I'm considering this to be a regular maintenance task expected of the SCCM Service Team and not something that this Committee needs to vote to approve. *[after further information was provided, this isn't as minor as originally thought -- requiring, potentially, a 24hr degradation of the service which would affect software installations for example. this updated information was provided to the committee]*

  As the announcement of the update will note, OU Admins will need to update their SCCM consoles to a new version, but we'll see about pushing that upgrade out. If not, its a minor inconvenience for OU Admins to update it manually.

  However, the second part of this upgrade will require a new SCCM client/agent to be pushed out to all of the workstations. Initial testing indicates that this does not require a reboot of the workstation, and as such, shouldn't impact the end users. But, as it touches so many boxes, we're erring on the side of caution.

  The AD Technical Committee has recommended that this part of the upgrade be pushed out to July 1st so we'll have completed the Kaspersky client upgrades and there shouldn't be any overlap in the two upgrades.

  Are there any questions from the AD Policy Comm? Issues with the date? Suggested alternatives?

**ACTION**: Committee Approved 5/29/14. SCCM Core Team notified.

=====

**Agenda:**

**August Meeting Change of Date**
August Meeting Moved from 8/15 to 8/22.

**Highlights from AD Technical Committee [Dan Green]**

- Domain Controller Event Log Issues resolved (sortof)
    - Derek has the old mechanism working again. However, the speed at which the AD logs are now rolling over is shorter than it takes to export them. So we're losing some.
- DirectAccess -- proof of concept is working within WolfTest. Requires a discussion with ComTech before it can be made production as it will impact the usage of the campus VPN system.
    - Meeting occurred, pilot in WolfTech has been approved. Management, bootup, and login are the functions that are being focused on -- so computers will be allowed to talk to wolftech.ad.ncsu.edu infrastructure servers (must end w/ that DNS domain).
    - Accessing other machines (file servers, license servers, desktops, etc, won't go through Direct Access -- VPN will still be required.
    - Test machines will need to turn back on and configure IPv6.
    - Michael Underwood will be leading the pilot.
- New Pregenerated NCSU level "people" groups.
    - All NCSU Faculty and All NCSU Staff already existed.
    - Now All EPA Staff, All Students, All Ugrads, All Grads, All "other" students available as well.

**CED Service account addition to NCSU-Read Group Memberships [Meimei Davis]**
Request to add College of Education service account "CED.owncloud.service" to the "NCSU-Read Group Memberships" AD security group? In CED, we would like to configure LDAP authentication for our new Owncloud system. And in order to manage our Owncloud users group, this service account will need the appropriate permission to access the "memberOf" attribute of WT Managed Groups.

ACTION: Committee Approves.

**Status of SCCM Service [Gene Morse]**
There's been a number of issues that have come up (and are continuing to be discovered) after

the SCCM service upgrade on June 3rd. Gene will provide updates and answer questions.

SCCM client upgrade still needs to be upgraded -- still planned for July 1st. That upgrade will force a full HW/SW inventory. We need to change the required upgrade from 1 day to 2 weeks to space things out. Following the upgrade, there will be a secondary SP1 patch that will be applied as well.

Gene: upgrade went fine, but we had some issues with backlogs that needed time to resolve. Then Kaspersky was installed on the servers, which caused a massive backup due to the way that Kasp was scanning on the servers. Backup was resolved and discovery was turned back on again.

Michael: further tweaking of the discovery process and reboots seems to have resolved more issues. Full group discovery now takes about an hour to run (there's a 30min process that occurs after) -- so 1.5hrs in total from the end user standpoint. If it keeps at this, we'll lower the 4hr cycle to 2hr cycle.

We also unchecked the box for "Discover objects within Active Directory groups" in the User and System Discoveries that were causing major duplication of DDR objects due to computers that were in tens of SW groups.

Current schedule:
8pm -- full system discovery
10pm -- full user discovery
2am -- full group discovery

Patching Issues Discovered. Microsoft patching group was 150GB in size and every 4 hrs, it was trying to push out to the distribution points. Adjustments have been made, but more need to be made…

Thinking of start creating a monthly deployment group to try and reduce the size of the patch files so the DPs can get them faster.

NOTE: A newer version of the SCCM "Right Click Tools" will also be released out to the OU Admins shortly.

SCCM Imaging -- still "wonky" but testing continues to resolve the service issues. In the meantime, keep using WDS. As there was an alternative, other SCCM issues took priority.

**SCCM Hardware Inventory Scanning [M. Underwood]**
Request to change the SCCM client setting -- increasing our hardware inventory from 5 days to once every 24 hours. AD Technical discussed during their last meeting and didn't have any objections, but it was warned that the increase in frequency might shorten how long the SCCM

server-side logs are kept (historical records).

ACTION: Committee Approved. Announce and implement.

**Domain Group Policy Changes [Billy B]**
Billy would like to make multiple changes within Group Policy:

- "Always install elevated" needs to be turned off
    - historical base setting that allows anyone on a machine to run an MSI as system without any issues. Allows local users to install MSI based software on lesser managed environments. But it is a **security hole**. So request is to turn OFF as the domain policy and let OU Admins turn it back on if they want to allow this (currently, a number of OU Admins have already turned it off at their levels).
- Set delayed service startup (on application specific services) and ncsu-only firewall rules as defaults in ncsu-level packages
    - recommendation to change the default packaging guidelines so applications that come with services will delay the startup of these services until 180 seconds after bootup. **Doing this is a way of speeding up the time between bootup and the enduser logging in.**
    - Michael: how far do we go back? look at usage and use your judgement. if older package only have 5 assignments, move on.
- Turn off "Always wait on network" - forces synchronous GPO processing
    - **another way to speed up group policy processing on boot / login**. was being used to try and resolve issues w/ public profiles and software GPOs installations.

ACTION: Committee Approves and asks that a SysNews post be made and the changes implemented.

**Status of Kaspersky Rollout**
Discussion?

Major Environmental Changes since release:

- Software Monitoring turned off.
- Batch files not being removed -- or at least change heuristics from high to medium.
- Interaction w/ SCCM repairs.
- Email Monitoring (Outlook) turned off.

Migration tables / scripts have been updated so clients should be on the servers expected.
Macs joined to the domain will show up in your OU under the correct console.
Macs not joined will still go to the "other" server.

Some reported issues with the Dell "security point" stuff that comes with the preloaded laptops -- there's a Lenovo equivalent of it. Billy recommends looking at running with psexec (using the install as system option) for the non-domained machines that you're seeing this on.

Anyone still having issues should be directed to help@ncsu.edu and not directly to Joe.