AD Policy Working Group
Apr 17th, 2015
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, Payman Damghani

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

Guests: Billy Beaudoin, Derek Ballard, Anthony Workman

Business handled outside of meetings:

Remove certificate from Lenovo PCs associated with Superfish [B. Beaudoin, 3/19/15]
The recent issue with Lenovo pushing a bad cert to their machines, which can lead to a simple Man in the Middle attack, is supposed to be dealt with in the next microsoft malicious software removal tool. But it probably would be a good idea to set a GPO to remove the cert from being trusted.

What is Superfish? http://en.wikipedia.org/wiki/Superfish#Lenovo_security_incident

ACTION: Committee Approved 3/19/15. Request awaiting AD Technical group approval and then implementation by the domain admins.

NCSU-Read Group Memberships -> msds-memberOfTransitive [B. Beaudoin, 4/2/15]
Currently "NCSU-Read Group Memberships" can read the "memberOf" field on User accounts. That shows the list of groups the user is in, but not the list of groups those groups are in. In other words, memberOf does not recurse.

msds-memberOfTransitive was added in 2012r2 and does recurse. So it is much more useful for LDAP applications. AD is constructing that field on the fly as a summarization of all the group data. Its just a multi-valued string attribute that happens to have a list of all the nested groups. It doesn't even show any parent-child relationships, just a list of CN's.

I'd like to add msds-memberOfTransitive to the list of attributes that the NCSU-Read Group Memberships can read on User accounts in the People and NCSU OU's.

I want to add tokenGroupGlobalAndUniversal as well -- it is the exact same data as

msds-memberOfTransitive except it has SID's instead of CN's.

ACTION: Committee Approved 4/10/15. Request awaiting AD Technical group approval and then implementation by the domain admins.

Pushed April Patches to Late Group at Request of Security Committee [Payman, 4/16/15]
It is the recommendation of the Security Technology working group that MS15-034 be pushed out ASAP. This was a part of this patch Tuesday's batch of patches -- and as such, has already be released to both the early and normal groups in SCCM and WSUS.

Details of patch: https://technet.microsoft.com/en-us/library/security/ms15-034.aspx

A reboot is required to apply the patch so the committee voted to release all April patches -- rather than just this one -- so everyone only needs to reboot once.

ACTION: Patches pushed; see https://sysnews.ncsu.edu/news/551949df

=====

Agenda:

Patching During Adverse Weather [Jonn Perry]
With this winters/springs bad weather, the patching team has been discussing the patch schedule in regard to the Adverse Weather Policy and had a few questions.

Should patching be treated as an essential service during status 1 or 2?

Since the weather could limit testing, should the Early, Late or Normal patching schedules be adjusted during particular status events?

ACTION: Patches should be pushed as usual. If you have weather related problems, alert someone else on the team to push the patches. Alert Service Team to this decision.

Office365 Rollout and Testing [Billy/Derek for C. Cline]

Need to add a @ncsu.edu alias to wolftech UPN's in order for Azure AD to accept unityid@ncsu.edu as the login credential in Office365.

Need to test it in wolftest.ad first as we're not totally certain if this could muck up anything. Well, really, we're just confirming the process of adding/removing with Wolftest -- we can't really "test" until we go live on wolftech.ad. We believe it is very easy to add and to remove.

(Charles will be the one implementing)

One concern is future YFS design impact.
Technically, you could then login to your Windows box as unityID@ncsu.edu.

Problem… once we go live -- so that we can test it -- the Office365 folks will push to announce the service. If we have to pull it, the Office365 logins would die. So we need to make sure that they don't announce it as an public service until we've had *some* time to see if there's any issues.

ACTION: DanG needs to contact Franklin and Danny and explain the bit above. Otherwise, Committee approves -- confirm process on wolftest, then go live on wolftech.

AD / PCI Planning
Derek has started on OU structures; and a formal plan/schedule has been created. ComTech and Billy met regarding moving the DCs behind a private IP space and the firewalls (one more audit issue soon to be resolved!).

Site Boundaries in SCCM [M. Underwood]
We want to reconfigure the Site Boundaries in SCCM. Currently they are 0.0.0.0-255.255.255.254. We want to change them to align them to the same site boundaries in AD. So they would be:

10.0.0.0-10.255.255.255
152.1.0.0-152.1.255.255
152.14.0.0-152.14.255.255
152.7.0.0-152.7.255.255
~~172.16.0.0-172.31.255.255~~

The reason the site boundaries were so big was in SCCM 2007 to accommodate running of task sequences off campus. In 2007 you could only run a task sequence on the intranet, so the computer had to be within your Site Boundaries. In SCCM 2012 you can specifically assign task sequences to run outside of your boundaries. This change will have no affect on computers, end users, admins, or the ability to manage machines.

Once IP address scheme of PCI becomes more clear we will want to exclude those ranges from the Site Boundaries.

https://technet.microsoft.com/en-us/library/gg712679.aspx

ACTION: Approved, AD Tech already approved, and SCCM Admins now need to implement.

SCCM Reporting Point Update [M. Underwood]
We want to add the SCCM Reporting Point service account, OIT-SCCM.Report.svc, to the Windows Authorization Access Group.

In SCCM 2012 R2 they updated the Reporting Point to use Role Based Access Control. Now, when admins run reports they will only see results for machines they have access to in SCCM. Prior to this when admins ran reports they would get results for all machines on campus making reports no so useful.

In order to for the reporting point to determine what groups a .admin account is in it needs to be able to read the tokenGroupsGlobalAndUniversal attribute on user accounts. Currently the NCSU-Read Group does not have that ability. The only permission the Windows Authorization Access Group has on users accounts is Read on tokenGroupsGlobalAndUniversal attribute

Talks about what permissions the Reporting Services service account needs:

https://technet.microsoft.com/en-us/library/gg712698.aspx

Here is a quick summary of what the Windows Authorization Access Group does:

http://support.microsoft.com/kb/331951

And what the tokenGroupGlobalAndUniversal permission is:

https://msdn.microsoft.com/en-us/library/cc223397.aspx

ACTION: Approved, AD Tech already approved, and Domain Admins now need to implement.

Direct Access Update

- Kaspersky seems to still be breaking Direct Access. Problems being resolved / troubleshooted; something about Kasp breaking 443 tunnel. One scenario that MichaelU has found -- delay the start of KAV on the box (gives tunnel time to come up).
- Security & Compliance and ComTech wanted to test -- but the laptops were returned unused. There was concerns including logging details and looking at the traffic patterns. Payman has now volunteered to do this testing.

Both Michael and Payman going to try to push this forward.

Add Reporting Point URLs to the Trusted Sites list [M. Underwood]

http://oit100sccm-rp.oit.ncsu.edu/

https://oit100sccm-rp.oit.ncsu.edu

As another part of fixing the SCCM reporting system for OU Admins.

ACTION: Approved, AD Tech already approved, and Domain Admins now need to implement.

Reconfigure Discovery in SCCM to exclude the Domain Controllers container and the new Regulatory OU. Adjust login script for SCCM client installation appropriately. [M. Underwood]

Why? PCI compliance -- we're adding another primary PCI site. As a part of the PCI re-jiggering, we need to limit the scope of what the SCCM service looks at.

ACTION: Approved, AD Tech already approved, and SCCM Admins now need to implement. See http://sysnews.ncsu.edu/news/55352282

Identity Finder Update [Payman]
Project now being run by Kerry and Daniel; planned deployment of October? Plan is still to install on basically all machines.

Foreign Applications -- Do We Need to Pay Better Attention? [D. Green]

360 AV: http://www.360totalsecurity.com/en/
360 Browsers: http://www.360safe.com/

Brian Carty: "All of those are by Qihoo. I'm not sure if the browser is a separate thing anymore. It may just be packaged in with either of the antivirus products now. All of them are pain to remove because they're entirely in Chinese and tend to have multiple "are you really really sure you want to uninstall" options that will just reinstall it if you choose the wrong thing. Kaspersky seems to refuse to install if there's even the smallest remnant of 360 on a machine.

Qihoo/360 is the biggest issue right now since their product is an antivirus client. But I also see stuff from Sogou and Tencent on machines and I'm not sure how bad their stuff could be."

Discussion ensued and App Locker was suggested to blacklist the product at the dept level. Julie recommended that it be given to the Click Through Agreement process.

SCCM Default Images
Josh G: "How often does this get done?"
Michael U: "was only just recently done for the first time since October upgrade. Going forward? Quarterly, perhaps?"

Packaging Team Rights
Still need to address... Dan must read the email discussion, then figure out how to fix via ADTK.

Windows 8.0 and Windows 8.1 Baselines
Still haven't done. Derek has agreed to relook into this.

Email attribute changes in AD
Dan still sucks. Has not been implemented. Derek volunteering to do instead. But apparently, Tom is going to fight him for it.

SCCM Patching Timing [M. Underwood]
Michael wants to change the SCCM patch sync w/ Microsoft from every 4hrs to every 8hrs (3 times per day) -- why? Microsoft only releases new patches 3 times a time (this change will sync w/ them) and its been discovered that everytime we sync the server, it tells all of the clients to checkin and see if they need patches. So we're DOSing ourselves effectively for no reason doing it 6 times a day.

ACTION: Approved, sent to AD Tech for approval.

PowerOn Service Update [Dan E]
Also ready to go "live" soon. Apparently its currently limited to certain folks -- now all NCSU users will be able to make use of this. As a part of the release, they're working on a new design for the site.

SCCM and MBAM [M. Underwood]
Michael wants to make a change to SCCM/MBAM policy -- if SCCM initiates a reboot of a computer, it will suspend the PIN requirement for bitlocker machines (those at the level that require the pin).

Committee: Only reason someone will even select to use the option of the bitlocker PIN is because they're forced to. Would this not break that compliance? Need to do more research… delaying an approval until Michael comes back having done more homework.