AD Policy Working Group
December 18th, 2015
3110 Engineering Building II
3pm-4:30pm

Voting Members: Donna Barrett, Charles Cline (remote), Dan Green, Julie Tilley (remote), Dan Evans, Daniel Henninger, Tom Farwig, Joshua Gira, Daniel Sink

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

Guests: Connie Reitfort, Andrew Kotynski (remote), Billy (remote), Debbie (remote), Brian Ott

---

Business handled outside of meetings:

SCCM Release of Updated Revision of KB 3097877 patch [M. Underwood]
KB 3097877, is an update to fix a security vulnerability in the OpenType font used in Outlook and Word. Since its release it has been causing Outlook and Word to crash unexpectedly. Microsoft has release a revised patch and expired the original. The revised patch has been released to the Early group, but probably needs to be deployed to everyone to fix the crashing issues that have been reported.

http://davidvielmetter.com/tricks/windows-update-kb3097877-breaks-outlook-and-winword/
https://support.microsoft.com/en-us/kb/3097877

I can't find anything from Microsoft that says they released a revised patch but I can see it in the Config Manager console.

It was probably deployed to the Early group on the 12th when it came out. I've rebooted my computer since then so I'm not exactly sure if it does or not. The KB article does not say a reboot is needed. Googling "KB3097877 reboot" only mentions rebooting if you uninstall the patch. On the description of the patch in the WSUS console it says "After you install this update, you may have to restart your system.", but I'm not sure if that's Microsoft default boiler plate you have to reboot catch all.

Discussion:

[Dan G] You're aware that all machines patching via WSUS have already received this patch, right? The WSUS server is configured to "Automatically approve new revisions of updates that are already approved" --- which could explain why none of our users reported issues. They received the new revision of the patch on the 12th -- technically, since it was released prior to

our Patch Thurs install schedule, they never saw the bad one (hurrah for Early/Normal/Late, that certainly worked out).

Recommendation (from Dan Green):
I'd say go ahead and push it. While this isn't an emergency security patch, for those affected, it is causing a business disruption. Plus in this specific case, there's a good chance that no reboot is even required. Unless you see folks on Policy saying otherwise, post the announcement to Sysnews/AD list at 11am and release it that evening.

I'd then instruct that the Patching Group to do the following:
1. Check to see if they couldn't update the SCCM patching rules/scripts to mirror the auto-approval for patch revisions that's already present/defacto in WSUS.
2. Failing the above, write a statement to address this scenario that we can add to https://activedirectory.ncsu.edu/services/patching/ under the section "Automatically Approved Update Classifications". Once approved by AD Policy, you'll not have to wonder about this when it occurs again.

Committee Approved 11/23/15. Patch was pushed, although notification was forgotten due to the holiday weekend. No-one appeared to notice.

=====

Agenda:

New Voting Member [Dan Green]
Welcome to Daniel Sink who replaces Payman Damghani as OIT Security's representative on the committee.

Jonn Perry has stepped down, Rob Blanke is new lead of the SCCM Patching service team.

[12/23/15 -- lists, google drive and google calendar invites updated to reflect both changes]

OIM and WolfTech AD [Connie Reitfort]
The OIM team is requesting approval for getting the IDM service accounts write access to OU=People at go-live (which won't be for several months). They don't want the access right now, but want to move through the approval process so that when go-live is scheduled there aren't any delays. They will be present to answer questions about this request and to find out what information they will need to provide to move forward.

Automated account provisioning to AD and others (Kerberos, OpenLDAP, Google, etc). And updating of the attributes (80 odd?) of these accounts.

Q: List of attributes (and what object class has been extended in AD to add those needed)? Brian will provide a complete list. And these are new ones that will be created (correction, already added via schema update):

> px OID 1.2.840.113556.1.8000.2554.999999.2.1
> lastpasswordchangedate OID 1.2.840.113556.1.8000.2554.999999.2.2
> oimpasswordexpirationdate OID 1.3.6.1.4.1.234.1.117
>
> Syntax Unicode
>
> This will be linked to the ncsuaccount class, which is the class used to designate Unity/IdM accounts.
>
> Attribute Usage:
> 1 - A calculation of PX and lastpasswordchange date will be performed to calculate the oimpasswordexpirationdate attribute.
> 2 - Shibboleth Service provider will be querying oimpasswordexpirationdate to determine password expiration

Q: OIMUSERS group membership? Concerns that a single group with 180K accounts in it might be a problem? Do we need direct membership or could we have subgroups (like we do w/ Unity Users)?

A: Old version needed all in one. New version seems to allow subgroups. Brian will confirm.

Q: Is there any change to how users are removed in AD compared to before? IE someone is gone for the summer, do they stay in Wolftech?

A: There will be a mass removal of student account who we've kept alive since Affiliates wasn't ready for them to move to. Plan is to go back 2yrs? Connie will confirm. When employee is terminated, 2-4 wks after they'll be migrated to affiliates; after the next tax season ends, they'll then be pulled from affiliates as well.

User testing has completed -- Debbie's team has confirmed that accounts can be correctly updated. Finalizing production environment of the system and doing final security testing.

Go live? No longer Feb. Not sure when. Will need the accounts configured a few weeks ahead of the date (once that's nailed down).

Service accounts have been created that will be used in production. But have no privs. Will only be given access to manage accounts -- will not manage groups at this time. So the scripts that we have adding people to Unity-A-etc… will need to live on.

During migration, Charles/Derek (Debbie's team in general) will be monitoring and will be the folks who can communicate w/ Connie's team should there be something fishy.

What is the rollback plan? Rollback? We don't need no stinkin' rollback. Go forward.

Preferred Name Project [Connie R.]
Students will have the ability to enter a preferred first name. Preferred name will be used in Unity and will be pushed out via openLDAP/Wolftech AD as the name used for their account. New "legal name" attribute will be added to Unity/Wolftech AD to house this information. What does this mean? If you have an app pulling firstname/lastname from either source, it will use the student provided "preferred name." If you have a reason to have access to the "legal" name, this will require special permission and a request will need to be made to get to it.

Hope to go live in January.

Rolling Identity Finder Domain-wide [Billy B.]
Identity Finder is required now for all merchants. It will at some point be requirement across all machines. It will only be scanning for SSN and CC#'s initially. There would need to be an exception process for some of the machines (though hopefully it would not be needed), where scanning would be stopped, but the agent not uninstalled.

Trying to figure out where the client needs to be installed is apparently a pain to define… hence, hey, let's install it everywhere and save ourselves some time. If it seems technically plausible.

There are current issues… client wants to suck up all unused processes on the machine. Which results in 100% CPU utilization (and if you're monitoring a server for this, you get notifications). And laptops don't play so well - they suck battery and turn into laptop grills. And scheduling can be a problem as machine might not be on.

Scheduled scans, seemingly, without local profiles created on the server per user will result in a full scan every time, not a delta scan. Currently the client is set to run twice a week -- Tues and Thursday.

Central file shares (think EMC NAS (please don't use the term "Celerra" as it is a long-deprecated product), AFS) will be scanned with special workstations that are configured to scan network shares. By default, regular workstations will not scan network drives. Departments running their own file servers will need to scan themselves (though if the server has the client, the discs are "local" for them).

VMs will also get the client installed inside the host.

Folks are looking at possible solutions -- like tying it down to a single processor core (which for newer machines would help -- not so much for older ones).

Billy is concerned that if we don't discuss and vote (knowing these still need to be resolved), then the governance process might negatively impact rollout. AD Technical voted the following: "Approved deployment across the domain with final implementation dependent on email confirmation from Jeremy and Michael of issues resolution/mitigation." Why the last bit? We want a technical person we trust to sign off that the issues have been resolved -- if not, then domain wide migration goes out the window, but then we'd need to go back to figuring out which clients need the software installed…

We'll have an "exception" security group that will allow us to have computers that don't need the client -- though S&C will need to sign off on adding computers to this group.

Dan E brings up a good point re: deploying campuswide -- does the licenses actually allow for us to install it on EVERY computer on the domain? Apparently we'll be providing it to students for selfservice… so we're thinking probably OK to install it everywhere.

Josh has concerns about it being installed on compute servers.

Michael has concerns about SCCM MP servers with all of the logs constantly coming in. Can we configure what the client scans on certain machines/servers? Yes, it's possible to create exceptions. Other instances to provide an exception for would be load balanced situations where all of the machines would be scanning the same data.

Can we get access to the data via APIs for reports.

AD Policy approves with the same caveats that AD Tech approved -- and note that communication out to the AD community must be made via Sysnews and email lists.

Further communication with the NCSU Software folks have noted that our licenses won't cover an across the board installation of this software… clarifications are being sought.

AD Service Accounts in LastPass [M. Underwood]
Can the policy committee mandate, if they so wanted, that all services accounts and passwords for all central AD services including SCCM/WDS/WSUS/Secunia must be stored in LastPass?

1. Does everyone have a LastPass? Most, if all, we're thinking. And its cheap ($14) if they don't.

2. Are there passwords that are too high valued to be placed in LastPass? Something that S&C would need to answer.

Idea would be to make sure that passwds needed for technical maintanance are in a location that all team members know. Brings together information stored in various text files, google drive, or spreadsheets… And survives someone leaving.

Daniel Sink has homework -- go back and get the answer to #2. If there's no issues -- and perhaps even better, encouraged by S&C -- then committee will vote on the issue via email.

Delegation of the NCSU OU [Billy]

Per the plan of splitting out permissions between Regulatory and NCSU, we have a goal to reduce the amount of Domain Admin use. A significant number of things are currently done at the NCSU level by domain admins (NCSU OU provisioning, NCSU-level software GPO's, resetting college-level OU admin passwords, college/dept renames, etc). So to help with reduction of attack surface and responsibilities of domain admin accounts, I'd like to propose a NCSU-OU Admins delegation layer.

As the meeting was breaking up, this topic didn't really get the discussion that it needed. Below is what AD Tech approved.

- NCSU-OU Admins
    - We need to create a permissions layer below Domain Admin and above current College/Department level
    - Responsibilities at this level:
        - New Delegated OU Creation
        - Creation and delegation of NCSU/Servers OU's
        - Assist in Package Promotion
        - Escalation point for GPO issues, .admin password resets, and so forth that currently goes to domain admins

Further discussion from AD Policy?

Would we put our .admin accounts in this NCSU-OU Admins group? Or are we talking about an .ncsuadmin account? Probably the latter.

See https://docs.google.com/document/d/1ByouwDAwBVbs2GgJbVAeqBEJpCwvqXZiEl3gjd_oXBY/edit for some thoughts on more things that need to have perms moved down to this level.

AD Committee: Concept seems sane -- now go figure out the specifics and report back changes. Present back before giving any individuals this permission.

Dropping the "EX" software naming convention [Michael Underwood]
The packaging team wants to get rid of using EX, since software seems to stay in EX, and any process improvements we've tried to implement have failed. "YES PLEASE" - daniel h.

Committee: Unanimously approved. Do it now. Warn OU Admins of the change and make sure they understand that SW/FW no longer means any sort of "testing" has occurred. Send out once prior to break and once after -- then start using new convention as of Jan 4th 2016.

Add HTTP MP and DP to SCCM [Michael Underwood]
There are thousands of machines with broken clients. According to the SCCM reports there are over 2000 machines that are having HTTP issues. Setting up a MP and DP that use HTTP instead of HTTPS may allows us to not only identify those machines but allow us to start managing them again.

The SCCM Core team is looking for approval to setup a HTTP MP for inventory and DP for patching of currently domain joined machines with broken SCCM agents. This will not be used to manage non domain joined machines.

These changes will have no affect on machines who currently have a working SCCM agent.

Committee: Approved. As AD Tech had previously approved, SCCM Core Team should move forward with implementation.

SCCM - Allow HTTP to support non-domain joined machines [Michael Underwood]
There has been a request to allow SCCM to manage computers NOT joined to the campus Active Directory domain. Example is transportation. Michael will facilitate discussion.

AD Tech approved installation of HTTP MP for inventory and DP specifically for patching of current domain joined with broken SCCM agents, but explicitly NOT for support of non-domain joined machines.

AD Policy is asked to weigh in on this.

[Update, prior to this meeting, it was conveyed that this request had been withdrawn by TSS]

Stuff on the horizon… (things not quite ready to be discussed)

- **DirectAccess Demonstration [M. Underwood]**
- **Security Standard for Sensitive Data and Systems [Jessie Henninger]** https://docs.google.com/document/d/1ZdLqnHmXZLKeYsPWXwM8l4XIn3fWmuf3nLQcE-0vYyk/edit#heading=h.ik9joinausi **Rescheduling for 2016 as Jessie left S&C.**