**AD Policy Working Group**
**August 21, 2015**
**3110 Engineering Building II**
**3pm-5pm**

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: Jessie Henninger, Will Ogle, Derek Ballard

---

**Business handled outside of meetings:**

**Direct Access Update [Derek Ballard, 7/20/2015]**
I've added "mrras.ncsu.edu" to the list of accepted DNS suffixes for WolfTech. Specifically, added it to the msDS-AllowedDNSSuffixes list.

Notes from Dan G: This domain will be used as a part of the DirectAccess infrastructure rollout (won't be publicly seen, but needed a URL separate from other current DNS domains on campus).

**AFS Client Upgrade Prep [Jeremy Brown, Billy B., 8/3/2015]**
I think we can safely uncheck the "Do not uninstall when falls out of scope" from the 1.7.26 package. It is the newest one out there at the moment. So it would handle the largest number of clients and the brokenness caused by the upgrade path would not apply to it because it is already the newest of the GPO-based installers.

Any problems with modifying just that package at this point? It will make testing and adoption of the new package easier.

Committee: Approved on 8/5/15; On 8/10/15, Billy B unchecked the "Uninstall when falls out of scope" on 1.7.26 and announced availability of 1.7.3202 package to the AD list.

**Emergency Upgrade of Firefox [Daniel Sink, Dan Green, 8/7/2015]**
Received from S&C via Daniel Sink: "Please execute emergency force upgrade protocols for Firefox. A vulnerability has been discovered in Firefox which allows a malicious javascript applet to be injected locally and steal sensitive files from a user's machine.
https://blog.mozilla.org/security/2015/08/06/firefox-exploit-found-in-the-wild/"

Per Michael's email, the Firefox AUTO package has been upgraded so new installs will be the latest version and he has changed the detection rules on the Deployment from 34.0.0.0 to 39.0.3 to get machines to start installing the new version.

As of 8/11/15, over 8,800 machines have upgraded with only 62 failures.

S&C wanted all instances of Firefox upgraded. We created a Collection that looked for all installs of Firefox with a version less than 39.0.3 and deployed the Firefox AUTO application to them. We were able to get an additional 1,200

**Upgrading SCCM to version 2012 R2 SP1 CU1 [Michael Underwood, 8/10]**
The SCCM Core team wants to upgrade the Site version on Wednesday August 12th to 2012 R2 SP1. This will allow us to manage Windows 10 devices.

During that time the site will be unavailable. It will require a console upgrade as well as a client upgrade. For those that have the console installed it will need to be upgraded before they connect back to the site. In the past we've done a force upgrade of all machines that had the console installed.

The client upgrade will come later, once we have the boot up script updated to install the new client. We'll also be using automatic client upgrades. This will cause a scheduled task to be created that will check for a new client. If one is discovered the new client will be downloaded up and installed automatically. In the past we've used a 14 day window. That means if a client discovers there is a new version available it will choose a random time between when the upgrade is discovered and 14 days out to automatically upgrade itself it the boot up script hasn't already upgraded them. And lastly we'll push the client to the WSUS server in SCCM. If the client hasn't been upgraded with the boot up script or the automatic client upgrade they will get a patch from WSUS that will cause them to upgrade their client.

This will give us three ways in which to upgrade the client. Once the site is upgrade we'll pick a date in the near future to upgrade the client.

We've already done this upgrade in Wolftest back in May or June with no issues.
https://sysnews.ncsu.edu/news/55c8e62a

AD Tech Committee approved site upgrade on 8/11/15. AD Policy Committee will be asked to approve the client upgrade at a later date.

=====

**Agenda:**

**ADMX Updates for Windows 10 [Derek Ballard, 8/5/15]**
I request approval to add the Windows 10 admx files to the WolfTech central store. http://www.microsoft.com/en-us/download/details.aspx?id=48257

Gives us Windows 10 specific settings in Group Policies.

I request approval to add/update the Windows 8.1 admx templates in the WolfTech central store. Honestly, i don't remember adding Windows 8.1 specific admx templates.

**Committee: APPROVED. https://sysnews.ncsu.edu/news/55f1c29b**

**Upgrading SCCM client to support new SCCM 2012 R2 SP1 CU1 [Michael Underwood]**
The SCCM Core team upgraded the Site version on Wednesday August 12th to 2012 R2 SP1. This will allow us to manage Windows 10 devices. https://sysnews.ncsu.edu/news/55c8e62a

The client upgrade must now be scheduled.

We'll be using automatic client upgrades. This will cause a scheduled task to be created that will check for a new client. If one is discovered the new client will be downloaded up and installed automatically. In the past we've used a 14 day window. That means if a client discovers there is a new version available it will choose a random time between when the upgrade is discovered and 14 days out to automatically upgrade itself it the boot up script hasn't already upgraded them. And lastly we'll push the client to the WSUS server in SCCM. If the client hasn't been upgraded with the boot up script or the automatic client upgrade they will get a patch from WSUS that will cause them to upgrade their client.

This will give us three ways in which to upgrade the client. Once the site is upgrade we'll pick a date in the near future to upgrade the client.

We've already done this upgrade in Wolftest back in May or June with no issues.
https://sysnews.ncsu.edu/news/55c8e62a

AD Tech Committee approved site upgrade on 8/11/15. AD Policy Committee is asked to approve the client upgrade beginning on **September 2nd 2015 if we are staying with the script, September 9th if we are going to use other methods to give us time to test new methods. Once the CU1 install is done, we will have to upgrade clients after that.**

SCCM Upgrade to CU1 and deploying the new agent.
https://technet.microsoft.com/en-us/library/Gg712298.aspx

**Committee: Go with old, tested method. Do CU1 first. Start deploying client on 9/2/15, use 5 day window to take advantage of holiday weekend. APPROVED.**

### NCSU Patching Standard Presentation [L. Howell, J. Henninger]

In order to be compliant with PCI-DSS the university must have documented standards for frequency and risk ranking of security patches. Thus, the document describes minimum requirements for applying security patches to IT resources that store, process, or transmit university data.

https://docs.google.com/document/d/1zaV-JBYDQU2mgLAhQuO0q75EgpE8caGOSYNUFS91p6Q/edit

The document describes a phased implementation to patch management, starting with the vulnerability management program for the cardholder data environment that is already being implemented, then prioritizing patching of IT resources that store, process or transmit sensitive data (per the Data Sensitivity Framework.)

In addition, the document:

- Describes how the university assigns risk rankings to security patches (pursuant to PCI-DSS requirements)
- Lists the maximum time allowed after a vendor releases a security patch that it needs to be applied, prioritized according to the data sensitivity level.
- Includes requirements for testing and rollback, and how to treat software unable to be secured.
- Explains how compliance is validated and who is responsible for validation.
- Explains procedure for exception to the standard.

Once published, the document will both reference and be enforceable under REG 08.00.02 - Computer Use Regulation as a university RUL on the PRR website. Effective dates in implementation timeline (§4) are the earliest enforcement can begin.

### Adopting Campus Patching Policy within WolfTech AD [Billy B]

In attempting to comply with the draft patching standard, would like to discuss implementing a stricter patching policy for the domain:

- Propose blocking the ability to disable Windows Update
    - couldn't really do via GPO - would really need to run scripts that alert us of those GPOs that disable patching and bug us or disable the GPO.
- Propose mandatory moving from legacy WSUS to SCCM for patching
    - Billy prefers that we instead announce a date to push everyone over to SCCM. Allow folks time to pipe up if they see issues.
- Propose 3rd party app patching no longer be opt-in
    - We're going to slowly ease people into this with some low hanging fruit.

Discussion: Does the committee support (and want technical implementation details) for preventing disabling patching AND force everyone over to SCCM? Yes, all agree this is the way forward. Come back w/ technical steps. If we approve, we announce to the campus community

(and governance groups above us) that it goes live in a couple months time so there's plenty of time for commenting and adjusting as needed.

- What if SCCM client broken? Point these machines at Microsoft (don't run local WSUS)
    - plus why are these broken in the first place? Michael has been investigating and believes that the boot script we're using might be breaking (running too many times?). Alternatively, should we ditch using the script and just use GPO or the SUP. Of the suggested ways of installing the client, scripting is last on the list, and even then it's a logon script not a bootup script. We are seeing a lot of broken clients. We've noticed even on healthy machines the client install seems to be running each time a machine reboots.
    -
- We're just talking about pushing patches -- we wouldn't control / force reboots. We could create suggested reboot time software groups if this would make things easier to manage at the dept level.
- How do we deal with exceptions? 1) Find the groups that have opted out so we can ask them why. 2)

**SCCM Data Storage Issues [Michael Underwood]**
Would like to set a policy on the number of version per application kept in SCCM to two.

For example there are multiple versions of Matlab in SCCM. We would delete and remove everything but the last two supported versions which would be R2015a and R2014b.

If users are trying to migrate from older versions to current they will have to create whatever applications or package that will be needed to help them do so. We want to do this in order to reduce the size of the DP's and to get a handle on the old and possible insecure software.

This would apply to all software except those where it is identified multiple versions are needed like Matlab. This would only apply to NCSU level software. Departments and College would still be responsible for maintaining their own software as long as there is space available on the DP's.

Committee:

- [Dan Henninger] What will the notification process be?
    - New version: Normal channels for testing/acceptance
    - Decom old version: Sysnews post with 1 week notice APPROVED.
        - will allow folks to respond and get copies for their usage, or if there's enough of a push back, we make an exception by acclamation.
- [Billy B] Is two versions enough? Go with 3 major versions instead. APPROVED.

**New Software Update Groups: Flash, Shockwave, and Pidgin [Michael U, Dan G]**
It's time to start piloting the usage of Secunia -- we'd like to start with these three apps: Flash, Shockwave, and Pidgin. We're picking these three as we feel we can say that one always wants the newest version -- if anyone disagrees, we can select an alternative.

Note that there will never be another centrally provided "version X" for these apps. Folks needing that will need to not be in the group and install themselves. But also note that we're starting w/ apps that this isn't likely to be an issue for -- that we'll tackle Java, etc once we have a proven working processes.

Explain that at the AD Pol meeting, the results will be discussed -- see changes in apps, report issues, etc.

At meeting we'll request that we move forward w/ dozens more (though probably not Java, etc). A month after, we should have enough backing us to go after the hard ones.

1. AUTO groups will be created for applications that will be patched through Secunia. There will no longer be version specific software groups created for those applications. The only way to get these applications installed will be through the AUTO group.
2. AUTO groups will be nested in NCSU-EX-Microsoft-SUP-AUTO
    a. This will change your WSUS server to https:\\OIT200SCCM-UP.oit.ncsu.edu:8531
        i. You will now get third party and Microsoft patches through SCCM
3. 3rd party patches will be deployed on the same patching schedule as Microsoft patches. On Patch Tuesday the newest version available in Secunia will be deployed to clients.
    a. There is no known API to automate the creation and publishing to WSUS
4. Collection Query rules will based on
    a. Targeted group: Early, Normal, Late
    b. Is your WSUS server set to https:\\OIT200SCCM-UP.oit.ncsu.edu:8531
    c. Being a member of the AUTO group

Question: How would SelfService groups work with this? Will need to create deploys for this as well.

Question: How about applications like Java where we'd need specific major versions?
While we're not going to include such an application in the early testing of the services, the plan would be for an Application to be created and deployed to the AUTO group for new major versions and Secunia will be used to patch minor versions. This would be useful with applications like Java.

- Version 1.0 - Application deployment
- Version 1.1, 1.2, 1.3, etc. will be installed with Secunia

## AFS to AuriStore (YFS) Migration; New Client [Billy B]

AFS client package (1.7.32) available for testing and AD list was informed. This package is a bit different from previous:

1. This may very well be the last OpenAFS client for Windows. The security changes in Windows 10 makes the barrier to entry for OS driver developers much, much, much higher. As such, the primary developer has already stated that they do not believe there will ever be a Windows 10-compatible OpenAFS client unless someone shows up with a wheelbarrow of money.

2. This client does not support Windows 10 and should not be deployed to it. If you need AFS, do not go to Windows 10 yet. Period. This new one is the only one that supports Windows 8.1 well, though.

3. There is a for-pay rewrite of OpenAFS (called AuriStor from YourFileSystem [YFS]) that we've already been looking at and will likely be licensing in the very near future. AuriStor will support Windows 10, but there are a lot of components that are just different enough that it may take quite a while to upgrade. It's also licensed based on the server environment and users, not client machines, so we'll see how the licensing shakes out. Currently the discussion is around having to collapse the number of AFS cells down to 1 (instead of the current 3).

4. The msi package is written completely differently than old AFS clients (its sorta based on the new AuriStor installer). Its just 2 MSI's instead of 3-5 plus scripts. For this reason (and for consistency) its being done in SCCM and not via GPO. Which means the whole upgrade process comes with caveats. One of which is we'll have to remove the "Uninstall when falls out of scope" from the NetIDMgr MSI on all the old GPO-based packages.

Most of this is just background for informed discussion. Force upgrading software would require approval from the committee (but can be talked about later once the package is fully tested). Additionally, statements about when to adopt Windows 10 probably should be talked about by the committee prior to anyone sending it out on the AD list, but will need to come very soon.

The intent is to force-upgrade current OpenAFS clients after the new one is fully tested and been out there for a bit. We'll need to have the old broken clients cleaned up before we will ever be able to move to AuriStor. There is about 1000 clients using the 1.7.1->1.7.24 packages.

There are a ton of the things that are broken in the older packages. We will likely have to enforce how we are doing all of the service discovery for AFS/Kerberos and normalize the configs before moving to AuriStor or that will be much bumpier than it needs to be. It will already be bumpy.

Also, once we make changes to the GPO's in order to help with GPO->SCCM move for the new one, it will break GPO->GPO moves from say 1.7.4->1.7.24 (not that it makes much sense to upgrade from an ancient package to a reeeally old one) since the MSIs will then be installed out of order. A brand new install of an old package would still work (but why would you?) but all upgrades, unless they are to the new one, will have issues. Which means we really need to kill the old packages. My preference would be to upgrade them and not orphan them.

Discussion:

1. Announce and force move from earliest 4 packages to v26 client. Why? Security issues with the even older clients and prep them for move to v32 later. Schedule it around the Fall break (Oct 8th). APPROVED -- Jeremy will post to SYSNEWS.

2. Once more testing of v32 clients has been made, announce force v26 clients to v32. Discuss this at the October AD Policy committee.

**Windows 10 Status Overview [Dan Green]**

By this time, Windows 10 will have been released to the public… believe we'll have Windows 10 Enterprise in place as well…

- KMS -- as of 8/20/15, appears to support Windows 10: https://sysnews.ncsu.edu/news/55ca6fb3
- Software Compatibility
    - Kaspersky [Joe Wells] - When Kaspersky announces support for Windows 10 by Kaspersky Endpoint Security 10.2.x, we will test it, announce the update and deploy the update if that is the mode the update takes. Until then, Kaspersky does not officially support Windows 10. See: http://support.kaspersky.com/kes10wks#requirements
        - http://support.kaspersky.com/us/12392#block1 -- "We plan to release Kaspersky Endpoint Security 10 SP1 MR2 for Windows Workstations and Kaspersky Security Center 10 SP1 patch D compatible with Windows 10 (Pro and Enterprise) before December 2015."
    - Cisco VPN -- http://ow.ly/QeyHk
    - AFS Client -- not supported until we switch to YFS client (see discussion above)
    - CrashPlan -- Windows 10 requires version 4.3 (we're running 4.1 currently): http://support.code42.com/CrashPlan/Latest/Getting_Started/System_Requirements
        - Everette has scheduled upgrade: https://sysnews.ncsu.edu/news/55df24ff
    - Alertus -- seems to function; Dan E mentions that an upgrade is also coming.
- RSAT for Win10: https://www.microsoft.com/en-us/download/details.aspx?id=45520
- WDS installations [Michael U]
    - We've added Windows 10 to the WDS server. Currently it is only 64-bit. We hope to have the 32-bit version soon.
    - With a new OS comes a new boot image. In order to install Windows 10 you have to use the WDS (Win10) x64 boot image. If you use the Default or any of the other ones the install will fail.
    - Also added a new driver group for Windows 10.
- SCCM client / software installs [Michael U]
    - Not currently supported, but there is work around for the SCCM agent. You can run the following command from an elevated command prompt with you .admin account:

      "\\wolftech.ad.ncsu.edu\files\ncsu\freeware\Microsoft-Configuration Manager Client-2012 R2 CU4\Client\ccmsetup.exe" /skipprereq:windowsupdateagent30-x64.exe

SMSSIGNCERT="\\wolftech.ad.ncsu.edu\files\ncsu\freeware\Microsoft-Configuration Manager Client-2012 R2 CU4\CCMsiteServer.cer" SMSSITECODE=WUF FSP=OIT100SCCM-AI.OIT.NCSU.EDU SMSCACHESIZE=10240 CCMDEBUGLOGGING=1 CCMENABLELOGGING=TRUE

    - We are looking at upgrading the Site version very soon, which will include a new client that is officially supported on Windows 10. https://technet.microsoft.com/library/mt131422.aspx
        - https://sysnews.ncsu.edu/news/55e0bf0f
- GPO Security Baselines [Derek B]
    - To address Windows 10 machines being joined to the domain, we have linked in some Windows 10 security baseline policies into WolfTech at the domain level. The policies are:
        - Windows10 Baseline Policy (beta)
        - WolfTech-Default Domain Policy - Win 10.0 (beta)
    - Each of these presently is just a copy of the Windows 8.1 security policies. When Windows 10 policies are available from Microsoft, we will upgrade to them.

**Discussion Regarding SCCM Site Boundaries [Daniel H]**

The site boundary configurations outlined here https://sysnews.ncsu.edu/news/553691dc appear to be effecting more than was originally expected. We are seeing issues where anything outside that boundary (the 172.* range we use for NAT'd installs in CHASS, and home addresses) are considered "unreliable network boundaries" by SCCM. I don't believe we should un-do that configuration, so we may want to put out a statement about it or document the behavior somewhere. The workaround is to set packages deployments and application deployment types to download anyway. Unfortunately it lumps "unreliable network boundary" and "slow link" together.  Remote folk can simply be asked to log in via the VPN to get around it. We (CHASS) could choose another IP range to use for our NAT setup that would fall within the 10.x range. There are a number of workarounds but it could be handy to make this a bit more known.

**Streamlining Certain Votes [Dan Green]**

We've had the general rule in place that pretty much all changes to the Wolftech AD require the approval of both AD Policy and AD Technical committees. I'd like to identify certain routine changes that have pre-approval by one of the committees and only require the vote of the other. The non-voting committee should be notified by email and the Chair should add the change to the "completed outside of meetings" part of their minutes (plus many will have associated Sysnews posts). The committees would still have the opportunity to question anything it saw as a redflag.

We would need to very explicitly define these, but at the same time, I think we might have some "rubber stamp" votes that we could automate.

Examples that I'd propose to begin with:

- Preapproved by AD Policy -- we need to know its happening, but really its the AD Tech

that needs to decide if this is OK:
    - Addition of Windows OS ADMX templates to the Central Storage
    - Adding of initial fill in the blank as no one is reading this
    - Updating the list of accepted DNS suffixes for WolfTech
    - Upgrades of Core Services to new versions by their Service Teams?
- Preapproved by AD Tech -- they need to know its happening, but really its the AD Policy that needs to decide if this is OK:
    - Read-Membership perms?
    - "Do not uninstall when falls out of scope" unchecking on software policies?

**Additional Domain Admin**
Jeremy Brown was voted to be a new Domain Admin in AD Tech. Vote needed. APPROVED.

**Quick Updates**
- MBAM - v2.5 installed Wednesday, SP1 applied Thursday. Still working on the web site interface permissions. Should have testing available soon --- limit your testing!
- DirectAccess - will refocus on it after MBAM completed. Looking to re-arch it a bit better w/ more redundancy.

---

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

**Yanking ffmpeg related applications... [Bill Coker]**
VLC…

**DirectAccess Demonstration [M. Underwood]**
[Punted from last meeting due to lack of time]

**Policies regarding creation and usage of .re accounts [Dan Green]**
[insert synopsys of last two meetings]

Further concerns within OIT have been raised, so Debbie scheduling a 2nd meeting to invite these folks to discuss proposal with domain admins. Want their questions answered prior to calling a vote in AD Policy.