AD Policy Working Group
October 16th, 2015
3110 Engineering Building II
3pm-4:30pm

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

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

Guests: Daniel Sink (remote)

Business handled outside of meetings:

Give oit.identityfndr.svc access to read People / Group Memberships [Payman D., 9/3/15]
S&C needs oit.identityfndr.svc to be added to the NCSU-Read Group Memberships for identify finder -- the campus' Data Loss Protection software that will look for SSN's and CC#'s on domained machines.

Committee: Approved 9/8/15.

Add Bitlocker ADMX files to the Domain Central Store [Derek B, 9/4/15]
The AD Policy committee instructed Michael to move forward with the MBAM (Bitlocker) project, but we didn't officially approve the addition of the Bitlocker ADMX files to the domain central store.

Just to cover our bases, I'd like a yea or nay from everyone please.

Committee: Approved 9/8/15.

Give renv-duo.proxy.svc access to read People / Group Memberships [Derek B., 9/8/15]
WOLFTECH\renv-duo.proxy.svc is a service account owned by OIT Security and Compliance. It is being used to provide proxy authentication services to the Duo two-factor auth mechanism. S&C desires to provide this service to all AD accounts (for example, to .admin accounts).

We request that it be allowed to place this service account into the "NCSU-Read Group Memberships" group to facilitate this.

Committee: Approved 9/9/15.

Add additional SCCM Inventory Pieces [Billy B, 9/22/15]
What do people think about adding the registry keys under here to the SCCM inventory? HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results

These are last Detect, Download, and Install times for patches from the Windows Update Agent. It works for clients talking to WSUS or SCCM (though the SCCM times are last time it downloaded the .cab file).

This will make it a little easier to answer the "what clients are not patching" based on SCCM inventory data than using some of the current inventory components (going through all of QFE install times and choosing the latest).

(this will either not include Windows 10 or we'll find the equivalent key locations for that OS and include them later)

Committee: Approved 10/14/2015

Extend SCCM Inventory [Michael Underwood, 9/23/15]
People have asked in the past if there is a way to inventory the members of local computer groups, and out of the box there isn't.

Sherry Kissinger, who's a big time SCCM guru, has a great way to inventory the members of all local groups on a computer so a report or query can be written. It use Configuration Baselines to collect the members of local groups and writes them to WMI where they are then inventoried. She provides a download for the Baselines and the mof file to extend the inventory

http://mnscug.org/blogs/sherry-kissinger/244-all-members-of-all-local-groups-configmgr-2012

I tried it in WOLFTEST and it works great. This is the information for engr01sccm:

Account	Category	Domain	Name	Type
Domain Admins	Group	WOLFTEST	Administrators	Domain
local_	UserAccount	ENGR01SCCM	Administrators	Local
OIT-Servers-SCCM	Group	WOLFTEST	Administrators	Domain
OIT-Servers-SCCM-Admins	Group	WOLFTEST	Administrators	Domain
agerber.admin	UserAccount	WOLFTEST	ConfigMgr_CollectedFilesAccess	Domain
Domain Computers	Group	WOLFTEST	ConfigMgr_CollectedFilesAccess	Domain
OIT-Servers-SCCM-Console-Admins	Group	WOLFTEST	ConfigMgr_CollectedFilesAccess	Domain
Guest	UserAccount	ENGR01SCCM	Guests	Local
agerber.admin	UserAccount	WOLFTEST	SMS Admins	Domain
Domain Computers	Group	WOLFTEST	SMS Admins	Domain
ENGR01SCCM$	UserAccount	WOLFTEST	SMS Admins	Domain
OIT-Servers-SCCM-Console-Admins	Group	WOLFTEST	SMS Admins	Domain
OIT-Servers-SCCM-Users	Group	WOLFTEST	SMS Admins	Domain
ENGR04SCCM$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_MP_WUT	Domain
ENGR05SCCM$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_MP_WUT	Domain
WT-SCCM-03$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_MP_WUT	Domain
ENGR04SCCM$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_Stat_WUT	Domain
ENGR05SCCM$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_Stat_WUT	Domain
ENGR06SCCM$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_Stat_WUT	Domain
WT-SCCM-01$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_Stat_WUT	Domain
WT-SCCM-02$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_Stat_WUT	Domain
WT-SCCM-03$	UserAccount	WOLFTEST	SMS_SiteSystemToSiteServerConnection_Stat_WUT	Domain
Authenticated Users	SystemAccount	ENGR01SCCM	Users	Local
Domain Users	Group	WOLFTEST	Users	Domain
INTERACTIVE	SystemAccount	ENGR01SCCM	Users	Local
OIT-Servers-SCCM-Users	Group	WOLFTEST	Users	Domain

The Baseline is written to exclude domain controllers. Baselines also run on a schedule. In Wolftest we have it set to run at least once a day. In Wolftech I think that might be a little aggressive, and would dump a ton of data into the database. Of course the more often you run it the more accurate the information is. This should not use this if our desire is to get real time information. We can start running it once a week and see how large the database grows, and if it's not a big we can run it more often.

Committee: Approved 9/24/15.

Agenda:

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.

Committee: [Michael U] Please update the packaging docs to include the correct boxes to be checked so we don't run into this on new apps. Anyone else running into it should report the issue.

Local Administrator Password Solution (LAPS) [Billy B]
"Microsoft released the Local Administrator Password Solution (LAPS) earlier this year, and we strongly recommend that enterprises deploy it to workstations and member servers. LAPS is a simple and elegant solution that randomizes local account passwords so that no two computers on your network have a matching local account and password. When computers have identical local account passwords, an attacker who gets administrative rights on one computer can easily take over all other computers on the network via a pass-the-hash attack. LAPS mitigates that threat. The Windows 10 baseline includes policies to enable LAPS. (Note that LAPS requires an Active Directory schema extension.)"

Details: https://technet.microsoft.com/en-us/library/security/3062591.aspx

Some groups on campus are already doing one form of this or another -- but we don't have a consistent domain wide approach. Penn State had a hack where one infected box managed to hack all the rest as they all had the same local admin password. We need to take steps to avoid this.

Suggestion is to make use of this as a default (allow folks to opt out). We would need to extend the schema so the information is stored there. Would set it to change every 30 days (well, would have it match the computer object password change schedule which is currently 30 days). Can make use of the FGPP system - but we'd use the same settings that are currently in place for local accounts. There's a MSI that we'd also need to push out that installs a dll file in computer to make this work. We also need to add ADMX files so we'd have an interface to view the password.

Who can see the password? OU Admins would have it by default. Units would have the ability to grant access to other security groups as needed. One units' OU Admin would not see the passwords for other units' computers. Machines would not change local admin password if it can't talk to the domain (to update the stored password).

There appears to be the misunderstanding that we're already scrambling the local admin password and throwing it away…. should see if we can track down that.

OK, so who's going to do it? Billy volunteered to implement.

Committee: Based on the above recommendations, Committee approves and asks AD Tech to review/implement.

DRAFT Security Baselines for Windows 10 released [Dan Green]
"Microsoft is pleased to announce the beta release of the security baseline settings for Windows 10 along with updated baseline settings for Internet Explorer 11. With this release we have taken a different approach from baselines of the past. Instead of piling on more settings and continuing to grow the size of the baseline, we have reevaluated older settings to determine whether they address contemporary threats, and have removed 44 (so far) that don't. In many cases, these settings merely enforce defaults that don't need to be actively enforced through Group Policy. By removing these settings, we allow administrators to focus on real security issues, and allow organizations that choose to enable a technology or feature to be able to do so without having to argue with or receive failing marks from security auditors, or to reverse group policy settings."
http://blogs.technet.com/b/secguide/archive/2015/10/08/security-baseline-for-windows-10-draft.aspx

Question: Should we be using these instead of the beta baselines (copies of the Win8.1 baselines) that Derek added to the domain back at the end of August?

Most of the Windows 10 install base appears to be mostly IT folks (76 Win10s currently on the domain). Do it now vs later.

Committee says, do it.

Windows 10 Current Branch for Business [Billy B]
(FYI -- All NCSU students can get Windows 10 for free. Not sure it was announced. Not Dreamspark related -- see http://ncsu.onthehub.com. And this version is the "Education" version, not the Home version. So students could use Bitlocker on this version.)

MS plans to release large service packs every few months -- that's the new Service Pack approach. This will be released via regular Windows Updates. We have the option to ignore these SP bundles -- or at least bump it until the next one.

Current Branch -- you get patches and service packs as they release.
Current Branch for Business -- you defer once, so you get the security patches per normal and download the SPs, but it will be 4 months after SP release before it gets installed.

Recommendation -- we set the default domain to CB for Business and then create an OS application/security group for current branch that we recommend OU Admins put their machines in there (or all of their Early group if desired). Need to post this out to AD list and Sysnews.

Committee Approves.

Mandatory Patching Revisited [Billy B]
https://docs.google.com/document/d/1ugRHNg_7WDeuz3WBdzFQiR_93QYvnOFCPl66qhj-PhM/edit

Decision for AD Policy -- by default, do we merely prompt that a reboot is needed, or do we reboot to make sure machines w/ poor administration do get patched?

- Set to not reboot by default, but nag on machine that reboot is needed (by default).
- Create some standard “reboot” groups -- nightly, Sunday night, once a month.
- Create a high-level security group whose membership is approved by S&C (aka, go talk to them if you have a computer that cannot be patched and wish an exception to the campus patching policy) that is set to ignore/deny to these policies.
- Show in Software Center so folks can initiate patches for the Late Group (aka, mostly servers).
- (suggested) Some report that informs us of computers that haven’t rebooted in 30 days

Revisit in 6 months to see how the compliance has been and if we should change the reboot or not default.

If approved, then Billy will go off and get the technical implementation completed. Then there will be an announcement to the OU Admins / SysNews post prior to the switch being flipped.

Committee Approves.

Update on yanking ffmpeg related applications... [Dan Green]
VLC saga continues… The following was passed along by Bill Coker.

==========
Per our discussion yesterday, we in OGC believe that given the complexity of and uncertainty about the legal issues involved with VLC and LAME, it behooves us to further investigate those products. In the meantime, NC State must continue to maintain robust cyber security by deploying patches of these products when available. NC State deploys these patches not to encourage or approve use of these products, but rather to protect its systems and assets, given our awareness that such products are being used. The patches are in no way intended to be indicative of our endorsement of these products or reflective of a legal opinion that such products comply with applicable laws. We intend to investigate these products in order to gather additional information regarding potential legal issues with their use, and will keep you updated with our findings.

Thanks,
Brent
--
Brenton W. McConkey

Assistant General Counsel
North Carolina State University
Office of General Counsel
==========

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 (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. So Billy will start an email discussion for it.

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

DirectAccess Demonstration [M. Underwood]
DA system was put aside for BitLocker implementation.

Policies regarding creation and usage of .re accounts [Dan Green]
Dan still needs to type calling a vote in AD Policy.