**AD Policy Working Group**
**Feb 20, 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

---

**Agenda:**

**Microsoft OnSite Engagement - AD security review [Dan G / Billy B]**
WolfTech Domain Admins are working with Microsoft staff on site to do a routine audit of the Active Directory domain and the domain controllers. This was conducted Monday-Thursday (January 26th-29th). There are some changes to the domain as a part of this process.

- Increasing Security Log size and enforced consistency in log settings on all DC's
- Removed historical, but disabled, accounts with domain-level access
- Applied MS baselines on domain controllers with respect to location of sensitive accounts, enforcing authentication standards, and interaction with removable media
- Enabled periodic vulnerability scanning of domain controllers

We still need to post the report on the AD website (privately).

In summary, about 1/3rd of the issues were campus wide issues / policies, another were minor things / cleanup, and the final items were in progress / needed changes to the domain that we can / need to tackle (many for PCI requirements).

**SCCM 2012 R2 CU4 Upgrade [M. Underwood]**
SCCM 2012 R2 CU4 has come out. We are currently running CU2. We are doing the upgrades in Wolftest on Tuesday Feb. 24th. If all goes well we want to proceed in Wolftech starting on March 9, which is the first day of Spring Break.

Impact: Based upon the last upgrade, people will have to upgrade their consoles before they can connect. There should be no issue with an older agent talking to a newer site. As before we will be using the Auto Upgrade feature to upgrade the clients over the course of 2 weeks. We'll also change the start-up script to install the newest version. We'll have more definitive answers after we do the upgrade of Wolftest next week.

Why do it? Keeping up to date and the hope to avoid / resolve bugs that we're not aware of. Gains us new powershell commandlets and being up to date is one of the first requirements of getting MS support when we do have problems.

http://blogs.technet.com/b/configmgrteam/archive/2015/02/02/now-available-cumulative-update-4-for-sc2012-r2-configmgr.aspx

Billy suggests moving the upgrade to the Thurs prior to Spring Break rather than the Friday to give a day in case the upgrade goes kaplewy.

Committee: No objection to doing the upgrade over Spring Break and shrinking the client reinstallation window from 14 days to 8 days (so entire process is completed by the end of Spring Break).

**Microsoft BitLocker Administration and Monitoring (MBAM) [M. Underwood]**
We have a working proof of concept for MBAM, Bitlocker administration and monitoring, in Wolftest. We want to move forward with setting one up in Wolftech. We've already talked to the Security Subcommittee about recommended GPO settings. It won't require anything to be changed for the domain.

Details on MBAM:
http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/mdop/mbam.aspx

Current practice requires OU Admins to create group policies to set and then have to manually tell the machine to encrypt the harddrive.

Need:

1) Agent on workstation(s)
2) Web server (help desk and self-service have separate sites) which talks to the
3) Database server which keeps the keys
    a) helpdesk could be given access to keys to allow them to assist users to unlock, but by default they can't see the reports
    b) "advanced helpdesk" (aka S&C) would have full access to everything without all fields filled in.
4) reports group -- allows users to see who has the agent, who's encrypting, details on the machines.
    a) Currently no federation within the server, so all keys are available to all who can log in; still need hardware ID from the user (or pull HW ID from AD object)
5) There is the possibility of a self-service for endusers as well.
6) Agent will encrypt harddrives w/o enduser intervention.
7) Two levels of encryption - whole drive encryption and encryption with boot-pin (for

those with red/purple data) -- 8-24 ASCII character pin (which is required to be created after 14 days). Can switch between encryption services though it does take time.
8) For those that require pins, there is a method to suspend bitlocker, reboot, then reinitiate bitlocker -- will allow folks that need to reboot, patch, etc, a way to not have all of their machines sitting at this prompt. But not simple.
9) If the laptop dies, you do still have the option to remove the drive, connect it to another machine, then use a security process to unlock the encryption to allow transfer of the data.

This will also make removeable drives less dangerous to encrypt -- currently, the keys for these are associated with the computer object that they were connected to when encrypted. This new service would escrow the keys for these drives with the central service instead -- so you could get a new computer, delete your old computer object, and not lose the removeable drive encryption keys.

Machines without TPM chips will not be affected.

Will run on 4 or 5 VMs. 2 GPOs that will need to be added to the route of the domain -- well, in the new PCI world, we'll link at the NCSU level.

Who will be responsible for the servers? So far its been M. Underwood and Tim Smith (TSS). Probably need to move it under the SCCM Core Team or Domain Admins. Someone will need to provide longterm feeding and care.

Committee: We need to **move forward** with this. But want an owner to be officially selected. And we want to know more details on the enduser self-service option before it goes live (OIT Security & C needs to also review this element prior to its use; they've signed off on the rest).

**Windows Proxy Auto Discovery [B. Beaudoin]**
The security subcommittee last month requested that Windows Proxy Auto Discovery (WPAD) be disabled in WolfTech. WPAD allows you to create DNS records that tell Windows clients where proxy servers should be based on DNS zone. We don't use it and never have. However, it can be used to create man-in-the-middle situations if it is enabled on a client but the DNS records don't exist (particularly for mobile devices that are hitting some else's DNS servers).

Affects: Will very slightly increase speed. And make it more secure! NCSU has never implemented the service, so turning off should have no ill effects. This will disable it in AD and a WPAD DNS record will be created that non-AD Windows machines on campus will see/use.

Committee: Approves, sending to Technical comm to review prior to implementation.

**PCI Update**

Billy's plan for PCI compliance appears to have been accepted as gospel; quite possibly due to the fact that no other plans have been proposed. Was noted during the recent meeting that new reinstallation processes will not allow us to reinstall payment workstations "in place" -- you must provision as you'd normally do, then deploy. If reinstallation needed, would need to pull back in and reinstalled/reprovisioned… this is critical to keep the **existing** reinstallation systems (WSUS/SCCM) out of scope!

Will need to have a strict division between the NCSU OU structure and the rest of the domain. Well, technically between services that admin the domain and admin machines / accounts within the NCSU OU. A number of services within the OIT OU will need to be pulled up into a more central server OU.

Stuff we'll need to duplicate -- AGPM, SCCM, SCOM, Kaspersky, and others.

**Packaging Team Rights**
Still need to address...

**Windows 8.0 and Windows 8.1 Baselines**
Still haven't done.