AD Tech Service Team Minutes 7/22/2016, PA-109-ENGR

Members: Alan Surrette, Billy Beaudoin, Charles Cline (chair), Joshua Gira, Derek Ballard, Dustin Duckwall, Fred Eaker, Jeremy Brown

Present: Jeremy Brown, Derek Ballard, Alan Surrette, Dustin Duckwall, Fred Eaker, Billy Beaudoin, Josh Gira
Absent: Charles Cline (chair)

Guests: Gene Morse, Dan Evans, Abraham Jacob, Joe Wells, Dan Green (remote), Rob Blanke, Carol Hill

Approval of minutes from 6/17//2016:
https://docs.google.com/document/d/1wAtkY2aWN6_wiih9bLSnXNBZrG-LSSJrXiMpiTW4Ib0

Notes from Last Policy Meeting:

Voting Items:

- Charles Cline's last day is 19 August. He is on vacation till then.
    - How do we handle his chair replacement
        - Holding off on electing chair until Susan speaks to Dr Hoit
        - Electing an interim until 19 August 2016
            - Interim is Jeremy Brown
    - How do we handle keeping an appropriate amount of votes
- forthcoming WolfTech schema update for "ncsuPrivacy" attribute (Derek)
    - Vote passes for updating the WolfTech AD schema
- Should we add more suffixes to DA to better support GPO Processing
    - Suggestion to make it by request.
    - Suggestion to do nothing and put responsibility on the dept admins
        - Choose to put do nothing and allow dept admins to make changes to their own NRPT. Michael will update activedirectory.ncsu.edu

New Items

- Page 21 is no longer a meeting space. We are looking for a new permanent location. Currently investigating some conference room space in SAS. If anyone has a place to volunteer we are open.
- Endpoint Protection Standard:
  https://docs.google.com/document/d/1M7Sxni5due7a2ajbMDnBJ1qb-Ys77qSQQcOLss8Fzjc/edit#heading=h.i2ao12fpb1ek
    - Presented to CITD last week

- The cron job for patching has been setup and seems to be working. Clients are being added to the group “NCSU-Active SCCM Clients” (See Action Items Reference) (Jeremy)
- Direct Access is fully functional at this point. Users should have access to all non DC VLANS via DA. Previously Connected clients were only allowed to access DC IP’s there were firewall rules disallowing outbound traffic. Traffic is now allowed outbound from the DA Servers to campus resources. The tunnel is still only valid for wolftech.ad.ncsu.edu . We can now use RDP, SMB to resources outside of the vlan. (Michael)
    - <DEPT>-SC-Microsoft-DirectAccess-OptIn
        - Enable Direct Access for machines
    - 35 machines currently in group
        - oitclients
        - Delta
        - CNR
        - CED
        - CHASS
    - Show logs
    - Should more DNS suffixes be added to DirectAccess to better support the application of GPO’s
- Windows 10 RS1 - 1607
    - https://blogs.windows.com/windowsexperience/2016/06/29/windows-10-anniversary-update-available-august-2/
    - There is an update that needs to be installed on the KMS server to activate Windows 10 Anniversary edition, which should also work with Server 2016. Might also need a new key
        - https://support.microsoft.com/en-ie/help/24717/windows-8-1-windows-server-2012-r2-update-history
    - August 2nd
    - Includes LTSB update - after this update, should only be patched once every couple of years
- MBAM
    - We have noticed on machines that support only TPM spec 2.0 when installing Windows 10 they must be imaged with UEFI inorder for Windows to take ownership of the TPM
    - Symptoms: Windows ask for the recovery key on every reboot even though no changes have been made
    - TPM Management console, verify that the TPM if fully owned and operational
    - Solution, disable MBAM or reinstall machine with UEFI
- Summer of OSD
    - starting to lay the groundwork to move imaging from WDS to SCCM
        - Will support legacy BIOS and UEFI
        - Will need new Mac Pool
    - If you are installing Windows 10 you should be using UEFI

        - There is a UEFI Mac Pool called WDS-UEFI
- When bringing up a Terminal Server, please submit a Service Now ticket to "oit_windows@help.ncsu.edu". Ensure that you have purchased appropriate Terminal Server licenses (thru Bill Coker)
- Enabling IPv6 on the domain has been completed. The GPO was set back to remove the key. Not to specifically disable. This means clients should go back to whatever their default state was.
- SCCM Endpoint Protection - server and role installed. Exceptions will go through S&C review, then linked in closest to requestor (i.e. CHASS, EAS, etc). (Michael)
    - 475 computers have been added to the software group
    - 16 pieces of malware on 41 machines
    - Currently not request to add an exception
- KB3159398, 1600 GP's might have issue. Recommend we hold patch for now, while we modify delegation script. Some departments that are not following conventions might need to deal with this outside of the delegation script (i.e. OIT). Jeremy and Derek own this process.
    - Daniel Henninger and Tom Farwig have expressed problems from this with Windows 10 machines in the AD chatroom
    - Per Billy:
        - Recommendation last meeting was to have <OU>-Computers:Read to all <OU>-* GPO's. https://github.ncsu.edu/Wolftech-AD-Automation/NCSUGpoDelegation/issues/3
    - Jeremy has updated the GPO script but it did not get updated in the cron. Need to take the current Github script and update the cron.
- Need to write down nomination process for Tech (and Policy?) Also currently no official quorum process. *Charles
    - Proposed:
        - Proposal for new voting members: 4 Domain Admins - 3 OU Admins - Policy Chair
        - all Domain Admins are voting members
        - The AD Policy chair is a voting member.
        - The AD Tech chair is a voting member (in both AD Policy and AD Tech)
        - CITD presents nominees; however, the AD Tech voting members vote the nominees into the voting members
        - Chair is elected from the voting members
            - Contention: Chair is vetted by voting members and should just be technically competent
        - Chair should be a voting member
        - Votes must win by ⅔
        - OU Admins = a user that owns a .admin account and actively supports Active Directory IT on NCSU
    - Additional things to be defined/clarified:

- What is the service owner responsible for exactly?

Action Items

Item	Assigned To	Date Due
Patching Discussion - To Policy	Billy	Approved in policy, Billy and Michael working on (waiting on Jeremy to setup a cron job Rob wrote)
Check Github permissions for DC's	Billy	

Action Items from Last Meeting

Item	Assigned To	Date Due	Status
Finish People OU permissions Audit and Cleanup	Billy		
Move ACLs that apply only to non-RegOU from the root of domain to NCSU and People	?		

Current Project Status:

- FERPA, confidentiality bit, etc (Billy and Charles) - IdM proposal to mask data. Possibly revisit c687c85 (identifier for userid). People OU perms still need to go through review.
- PCI update (Derek)

As part of the Regulatory/ PCI-DSS efforts, we decided to move the WolfTech domain infrastructure servers/services. Specifically:
From: wolftech.ad.ncsu.edu/Servers/<services OUs>

To: wolftech.ad.ncsu.edu/NCSU/Servers/<services OUs>
Derek looking for help thinking it thru & doing. Would meet outside the AD Tech meetings

- IdM (Charles) - Talks with new vendor (APTEC)
- AGPM update (Kevin)
- SCOM update (Kevin) - Demo?
- Directaccess (Michael)
- MBAM (Michael) - Demo?
- Use of Azure for virtual machines. Domain controllers, other types of servers/services?
    - Focus on getting connectivity first
    - Would need to be a real tennant, not tied to MSDN
- Domain Admin automation - Jeremy/Charles, reference doc is https://docs.google.com/document/d/1ByouwDAwBVbs2GgJbVAeqBEJpCwvqXZiEl3gjd_oXBY/edit
- Stuff we don't need to vote about, but still get notified. Examples?:
    - .admx added to central store for new Windows OS (should just be ok)
    - adding accounts to NCSU-Read Group memberships (Policy only)
    - New OS MS Security Baseline (put in asap with copy of most recent OS override)
    - Extending SCCM inventory?