AD Tech Service Team Minutes 8/19/2016, PA-109-ENGR

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

Present: Derek Ballard, Jeremy Brown, Dustin Duckwall, Fred Eaker, Billy Beaudoin, Joshua Gira
Absent: Alan Surette, Charles Cline
Guests: Daniel Sink, Gene Morse, Dan Evans, Michael Underwood, Adit Burkule, AJ Milton, Chris Betinni, Joe Sutton, Rob Blanke, Matt Pollard, E.C. Mabe, Robert Holleman, Dan Green, Abraham Jacob, Joe Wells

Approval of minutes from 7/22//2016:
https://drive.google.com/open?id=1nAVwk4jBRGsY3HLZEnVkmMLzUe61_eQBii4fsBKaU0g

Notes from Last Policy Meeting:

Voting Items:

- The next SCCM version (probably 1606) provides the ability to change cache size as a client setting. We would like to create a <Dept>-SC-Microsoft-SCCM-Set Cache 50GB
    - Should we increase the default cache size from 10GB to 20GB
        - If we increase to 20GB we should create a 10GB opt-in group
            - Vote passes to increase the default from 10GB to 20GB
                - Create opt-in groups before the change
                - Sysnews post to make the change
                - Change on 26 August 2016
- Jeremy Leaving ITECS - Domain Admin Account getting disabled
    - Need to write down and capture a formal process for employees moving into roles with greater permissions
- Jeremy is joining OIT - New Domain Admin!
- Vote on new AD Tech chair
    - Vote passed - Jeremy Brown is the new AD Tech Chair pending approval from ITSAC-I
- Auto-Approval of SCCM server and client upgrades
    - Add SCCM upgrades to the autoapproval list (which we've never finalized). Plan to move forward on your timeline, pick a date, and inform the comms. Give them a chance to object, but if nothing heard, move forward.
    - SCCM core team will test and then select a date for the server and client upgrades. They will announce these dates and give the committees at least 1

week notice. Should no objections be raised regarding the dates, they should proceed.
        - Vote passed - SCCM upgrades are auto-approved providing listed requirements are met

New Items

- Page 21 is no longer a meeting space. We are looking for a new permanent location. The SAS conference room we were hoping for fell through. If anyone has a place to volunteer we are open.
    - Following up on Scott Hall 216 as the new, permanent meeting space
- Endpoint Protection Standard: https://docs.google.com/document/d/1M7Sxni5due7a2ajbMDnBJ1qb-Ys77qSQQcOLss8Fzjc/edit#heading=h.i2ao12fpb1ek
    - Presented to CITD last month
    - Billy requests input in filling out the implementation guidance
- Upgrade SCCM to v1606. We have upgraded Wolftest successfully. We have upgraded the client .msi file in the GPO and upgraded the client on several machines successfully. We are hoping to upgrade the site on Aug 24th or Aug 31st. We would push the new client out around Sept 21st.
- 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.
- Direct Access documentation has been added
    - https://activedirectory.ncsu.edu/services/directaccess/
    - There is now a block with instructions for adding your own DNS suffixes to broaden to use of the tunnel.
        - You can add anything you want
        - DO NOT add *.ncsu.edu
    - Direct Access issues should have calls created in the SCCM Core team ServiceNow queue
- ITECS is hiring
    - https://jobs.ncsu.edu/postings/72998/

- Windows 10 1607 admx files now available
    - https://www.microsoft.com/en-us/download/details.aspx?id=53430
- IEtab admx/adml files (CVM/clbettin : INC2749476)
    - CVM has a product licensed via admx files
    - There is no adm file available
    - CVM will attempt to reverse engineer the admx file into a custom adm file
        - Billy will provide older, custom adm file he built if he can find it
- Windows 10 Current Branch for Business (INC2600326): Review and decide what the appropriate settings should be.
    - Early group should not be in CBB line
    - Normal and Late groups should be in the CBB line
    - Should there be an additional deferment beyond the delay created from enabling the policy as a default for campus
        - Determine whether the 4 month delay is hard coded?
- OITHS ou creation under OIT.
- Microsoft changing how security updates are distributed
    - https://blogs.technet.microsoft.com/windowsitpro/2016/08/15/further-simplifying-servicing-model-for-windows-7-and-windows-8-1/
- Powershell open sourced
    - https://azure.microsoft.com/en-us/blog/powershell-is-open-sourced-and-is-available-on-linux/
- S&C is looking to start the discussion about deploying a tool to campus machines for remote forensics. The tool we are investigating is GRR (Google Rapid Response - https://github.com/google/grr). It uses a control node and an agent on each machine (like SCCM, Tripwire, and other remote management tools).

  This would streamline our ability to collect forensics data from compromised machines - we could effectively fire off a memory capture remotely while drafting the notification to the affected parties. This would hopefully remove the need to ship around memory and disk images for analysis, and would let us remotely grab just the things we care about
- Temporary rights elevation of Wolftech to Azure AD service account wt.aadsync.sv (INC2752631) - ddballar
    - https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-accounts-permissions/
- 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?