AD Tech Service Team Minutes 12/9/2016, Scott Hall, Room 216

Members: Alan Surrette, Billy Beaudoin, Joshua Gira, Derek Ballard, Dustin Duckwall, Douglas Flowers, Jeremy Brown (Chair)

Present: Douglas Flowers, Dustin Duckwall, Jeremy Brown, Billy Beaudoin, Derek Ballard, Joshua Gira,
Guests: Gene Morse, Michael Underwood, Matt Pollard, Daniel Sink, Rob Blanke, Donna Barrett, Joe Wells, Abraham Jacob, Chintan

Approval of minutes from 10/21/2016:
https://docs.google.com/document/d/1cKwj3dAqbcGudKAuWj7WPwr7iSf_m_N9mGe_LLH4t_k

Notes from Last Policy Meeting:
https://docs.google.com/document/d/1-Pgo7CTVX-JCQSRMohJBXvsO5AZoFwaCBjet4WZ2Deg

Voting Items:

- AV Voting points
    - Can we remove the filter allowing the install of SCEP on Windows 7 and 8
        - Remove the OS filter for SCEP on 4 Jan 2017
        - Send vote to AD Policy for approval over email
            - Assuming AD Policy passes vote make a Sysnews post
        - **Vote Passes**
    - Can we make SCEP an opt-out instead of opt-in
        - Change the opt-in to an opt-out on 17 February 2017
        - Create opt-out group at least one week ahead of the hard switch
        - Opt-out needs to be -SC-
        - **Vote Passes**
    - Will SCCM (Site code: WUF) support machines that aren't in WOLFTECH AD?
        - Vote to only allow machines into SCCM/WUF if they also join WOLFTECH
            - If machines install the SCCM Client they will be targeted and joined to WOLFTECH into a "Single-User" OU that meets the controls on the Endpoint Standard and no more.
            - **Vote Passes**
- Laptop computer password changes
    - Vote to change all domain joined laptops to change their computer password every 180 days
    - **Vote Passes**

- Update DNS attribute via a cron job
    - Read NCSU-Macintosh group membership and set the DNS attribute on the computer object
    - **Vote Passes**
- Add the UID attribute (RID + 1 billion) to all user accounts not in OU=People
    - **Vote Passes**
- Request to create two OU's
    - wolftech.ad.ncsu.edu/Servers/PAWs
        - DomAdmins - Full Control
    - wolftech.ad.ncsu.edu/NCSU/Servers/PAWs
        - NCSU-OU Admins - Full Control
    - **Vote Passes**

New Items

- Windows 10 RTM Force upgrade
    - Microsoft is requiring Kaspersky (as a third party software) removal before Windows 10 can be upgraded
    - Folks who are doing in-place upgrades from older OS's to Windows 10 must uninstall Kaspersky in their task sequences first
- Kaspersky has been killed
    - AV Committee voted to not renew the Kaspersky contract. Our license ends on 28 February, 2017
    - VMware + Kaspersky scanning will stay for VM's in OIT's VMware environment
    - All domain joined computers are to use SCEP
    - Macs are to use SCEP
    - Non-domain joined devices are to join the domain or upgrade to Windows 10
    - S&C statement - All things Windows 7/8/10 can have SCEP installed
    - Communication needs to go out about VMWare. Users will need to make sure they put their VMs into the SCEP opt-out group
- With the Kaspersky change, how are we going to handle non-domain joined computers joining SCCM in order to receive SCEP?
    - Are we going to allow non-domain joined machines to join SCCM at all?
    - Are we going to auto-join them?
    - If we are, what level of support will they get?
    - How should the agent be installed on those computers?
- What are the pro's / con's about turning off the automatic password change for computer accounts for laptops. Goal is to stop the FUD about joining laptops to the domain.
    - Concern about pivot points from S&C rep for IT Admin laptops
    - Discussion about whether there is value in adding a date to kill the laptop over just letting them exist with no password change for the install lifetime of the OS
- Advanced Threat Protection
    - Moving from E3 to E5 will add ~200K/yr
    - At this time ATP is cost prohibitive

    - Possibly purchase for infrastructure machines
- Fix DNS suffixes for Macs?
    - If the DNSHostname attribute is missing it may be causing Kerberos issues with Macs
    - Do we programmatically fix the DNSHostname attribute or uncheck the box in the report
    - We need to investigate pulling the DNS Suffix out of the <Dept>-OU Policy since that is the authoritative data source
        - Get-GPRegistryValue -Name <GPO Name Derived from OU location> -Key "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\System\DNSClient" -ValueName "NV PrimaryDnsSuffix"
    - Mention about newer Mac OSes not updating the Operating System attribute.
    - Currently the cron job to update the NCSU-Macintosh group is looking for the Operating System attribute to populate the group membership
- Setting up One-way Selective Auth Trusts with other UNC Schools
    - shared stuff (like BME and Distance Education classes)
    - easier cross-physical disaster recovery potential
    - AD support issues
- Privileged Access Workstations for Domain Admin/NCSU Admin
    - https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/privileged-access-workstations
    - Request to create two OU's
        - wolftech.ad.ncsu.edu/Servers/PAWs
        - wolftech.ad.ncsu.edu/NCSU/Servers/PAWs
    - http://www.rebeladmin.com/2016/02/restricted-admin-mode-for-remote-desktop-connections/
- Moving Scripts and reports from Dan's stuff to AD attributes
    - Planning for the eventual decommissioning of ADToolkit in favor of more native tools (Powershell, AD Attributes, DisplaySpecifiers, Splunk, etc)
- Research Storage instructions are going out with information on how to join Linux boxes to WOLFTECH
    - https://docs.google.com/document/d/1viR8guyi5AECRRzU48i-kJogOuk2kTWPkBb_UxI7mJM/edit
- Add UIDs to all non-UnityID accounts (user account objects **outside** the People OU) in the domain, similar to what we did with the gids for groups (ddballar)
    - Suggestion is to mirror gid offset for uid's
        - RID + 1 billion