AD Tech Service Team Minutes 9/23/2016, Scott Hall, Room 216

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

Present: Billy Beaudoin, Derek Ballard, Jeremy Brown, Joshua Gira, Dustin Duckwall
Absent: Alan Surrette
Guests: Dan Green, Matt Pollard, Daniel Sink, Michael Underwood, Fred Eaker, Olivia Catlett, Jamie Dennis, Bert Stoner, Joe Wells, Robery Holleman

Approval of minutes from 8/19/2016:
https://docs.google.com/document/d/1pxXa-XBpH2pWVQ4q0gKCWmbXJLw0-5n_DL84f2Ypbjk

Notes from Last Policy Meeting:
https://drive.google.com/open?id=1jeZilAljFgHpFI0SXHgxMtWo_avpXkn4qV3UvWudYto

Voting Items:

- CITD has voted Doug Flowers (deflower) as the candidate to replace Fred Eaker.
  - **Vote passes**
- Roll out random MS patches for Windows 7 that improve networking and GPO performance
  - KB2775511 + some others
  - Proposal to deploy as a package instead of application model that way if it needs to be removed it won't be reapplied
  - Proposal to deploy to Windows 7 and Windows 2008 R2 SP1
  - It does require a reboot and will be deployed around a patch Tuesday
  - **Vote Passes**
- "Always wait for Network" -- everyone ignored Billy's nagging 2 years ago -- would like to script the removal of that setting from all GPOs
  - Is it a reasonable policy to edit GPO's en masse for making domain changes
    - As long as there is a Sysnews/AD list post providing ample notification
    - Delegating notification requirements for AD Policy to AD Policy
    - **Vote Passes** for making changes en masse (AD Policy sets notification requirements)
- Making separate client and server certs for computer certificate auto-enroll to make the client auth cert not tied to DNS.
  - Both certs will be deployed to all computers
  - Client cert uses SAMACCOUNTNAME
  - Server cert uses DNS
  - Current Computer certificate template gets renamed to the Client certificate

    - Server certificate template will need to be created new
    - **Vote Passes**
- NCSU Normal update target needs to be applied to computers not getting anything else
    - SCCM is looking for
    - regkey **HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate**
    - Item property **TargetGroup**
    - Need a setting applied to computers at NCSU to give a targeted group-normal
    - **Vote Passes**
- Possible change in the ldaps.wolftech.ad.ncsu.edu vIP; Derek wants the vIP to ensure that the vIP has "persistency" vs "round robin/least busy" setting.
    - **Vote Passes**

New Items

- Windows 10 RTM Force upgrade?
    - Windows 10 has moved into it's fourth version; however we have not enabled the Update from WSUS or SCCM for Windows 10 Upgrades. Technically we have computers that Microsoft isn't supporting anymore since they are only supporting three revisions back. Since the Anniversary update (1607) the RTM installs are no longer valid and should have been forced upgraded via Windows Update to, at a minimum, 1511.
    - The ability to enable the "Upgrades" option is still being worked on. There were requirements that had not yet been met. Expectation is that "Upgrades" will be enabled for October patches.
    - Early - Set to push 1607
        - NOT DONE YET: Semantics still needed for making sure the reg key gets set
    - Normal/Late - Set to push 1511
    - To find Windows 10 boxes: Get-ADComputer -Filter {OperatingSystem -like "Windows 10*"} -SearchBase "OU=NCSU,DC=wolftech,DC=ad,DC=ncsu,DC=edu" -Property Name,OperatingSystem,OperatingSystemVersion | Format-Table Name,OperatingSystem,OperatingSystemVersion -Wrap –Auto
- Report on RAP
    - https://activedirectory.ncsu.edu/wp-content/uploads/2011/07/2016_WDRaaS_Findings_Report.docx
    - https://sysnews.ncsu.edu/news/57ffa9dd
    - Move Domain-level Security Baselines to SCCM Configuration Items in order to avoid running 20 WMI queries on all machines.
        - Doesn't seem to be any pushback
        - Possibly need to look at changes to imaging since we will be delaying security application by a couple hours
    - "Always wait for Network" -- everyone ignored Billy's nagging 2 years ago -- would like to script the removal of that setting from all GPOs

- 'BME-OU Policy' -- 'Enabled'
- 'AEE-OU Policy' -- 'Enabled'
- 'BCH-OU Policy' -- 'Enabled'
- 'PPATH-OU Policy' -- 'Enabled'
- 'WQG-Patch Link' -- 'Enabled'
- 'OITLAB-Unity-Wait For Network at Startup and Login' -- 'Enabled'
- 'Design-Staff Desktops' -- 'Enabled'
- 'NCSU-SW-Autodesk-AutoCAD-2010-x86' -- 'Enabled'
- 'BTE-BIT0745-02 Logon' -- 'Enabled'
- 'COS-FW-Putty-.58' -- 'Enabled'
- 'BTE-Slow Link Detection-Wireless Labs' -- 'Enabled'
- 'CARM-Network-Startup' -- 'Enabled'
- 'OIT-Always-Wait-for-Network' -- 'Enabled'
- 'OIT-Always-Wait-For-Net' -- 'Enabled'
- 'COEDEAN-Testing Policy' -- 'Enabled'
- 'SHS-OU WS2008 R2 Policy - DO NOT COPY' -- 'Enabled'
- 'STUAFF-Startup Wait for Network-DELETE' -- 'Enabled'
- 'OIT-Servers-Citrix-Folder-Redirect' -- 'Enabled'
- 'CALSADM-Facilities-Billboards-Kilgore Power Schedule' -- 'Enabled'
- 'DASA-Staging-SystemLogon-AlwaysWaitNetwork' -- 'Enabled'
- 'CALSADM-Facilities-delay netlogon' -- 'Enabled'
- 'OIT-Servers-Citrix-Folder-Admin' -- 'Enabled'
- 'DASA-COU.Kiosk Logon Settings' -- 'Enabled'
- 'CSC-Setting-Wait for Network' -- 'Enabled'
- 'COS-capstone-quick' -- 'Enabled'
- 'CS-Wait For Network' -- 'Enabled'
- 'COS-Async-ProcessFix' -- 'Enabled'
- 'CS-Desktop Policy' -- 'Enabled'
- 'COS-Policy-Timeout' -- 'Enabled'
- 'DASA-SHS.Kiosk Check-In Auto Login Medicat' -- 'Enabled'
- 'OITHS-Always Wait for Network' -- 'Enabled'
-
- 'CS-OU Policy' -- 'Disabled'
- 'SSC-OU Policy' -- 'Disabled'
- 'ISE-Laptop Policy' -- 'Disabled'
- 'GIS-Fishbowl Default Policy' -- 'Disabled'
- 'ISE-Desktop Policy' -- 'Disabled'
- 'OITMD-EX-Power Plan Option' -- 'Disabled'
- 'OITMD-EX-After Hours Power Plan' -- 'Disabled'
- 'CS-Laptop Policy' -- 'Disabled'
- 'CALSADM-TestPCs-remove login delay test' -- 'Disabled'
- 'OITLAB-Test.Disable Allways Wait For Network' -- 'Disabled'
- 'OITMD-Clients-OU Policy' -- 'Disabled'

    - 'DASA-Network-Disable-Wait' -- 'Disabled'
    - 'DASA-UREC.Laptop-Disable-Wait-for-Network-DELETE' -- 'Disabled'
    - 'ISE-Teaching Labs OU Policy' -- 'Disabled'
    -
    - To Remove Setting:
        - Get-GPO -Name {Name From List above} | Remove-GPRegistryValue -Key "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Winlogon" -ValueName "SyncForegroundPolicy"
        - Or maybe better: Get-GPO -All | Remove-GPRegistryValue -Key "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Winlogon" -ValueName "SyncForegroundPolicy"
    - Do we keep nagging or blanket change every GPO?
        - If we remove it we can possibly make a naginator to email when re-enabled
- Advanced Threat Analytics
    - Gathering perfmon
- Advanced Threat Protection
    - Is included with E5, but we are at E3
    - Bill C. is working to see what we can do to get the ATP license added to us
- 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
- 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

- Research Storage instructions are going out with information on how to join Linux boxes to WOLFTECH