AD Tech Service Team Minutes 1/27/2017, Scott Hall, Room 216

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

Present:

Guests: Abraham Jacob, Joe Sutton, Gene Morse, Donna Barrett, Matt Pollard, Joe Wells, Kesley Mumpower

Approval of minutes from 12/9/2016:

https://docs.google.com/document/d/1JzHQMhcFuY06S5oMv3OYbzgot Zn4ibaZfh3lzNpEtQ

Notes from Last Policy Meeting:

https://docs.google.com/document/d/1J17OevfMRWbO0maCak2egyu6YzxfiYJycxTwpB2kx2Q

Voting Items:

- Can we remove the Important URLs from the Default Domain Policy?
 - o INC2035727
 - This functionality has been deprecated.
 - Approved 2015-11-16 by email
 - Vote Passes
- Give OIM service account write permissions on People OU?
 - Derek will email before the account is given permissions.
 - 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
 - V1507 "end of support", only ~89 machines still need to upgrade
 - If you have met the criteria AND it's been 31 days since you installed Windows 10 please submit a ticket to <u>activedirectory_patching@help.ncsu.edu</u> with the name of the affected machines.
- Terminal Services license server doesn't support Server 2016 currently. (Joe Wells)
 - There will be a new terminal server provisioned to support Server 2016.
 - Users will need to migrate their license server address to the new server.
- Software Updates

- By default nagging end users to reboot machines for patches
- NCSU-level (non-replicated) OptOut group for machines that are approved exceptions by S&C
 - This got forgotten in the patching changes made here: https://sysnews.ncsu.edu/news/57befcc9
- SCCM Upgrade to 1610
 - Need to set date for client upgrade Possible starting Monday Jan 30th
 - Reporting Point and Asset Intelligence were upgraded to Server 2016 as well during the SCCM upgrade.
 - New Reporting Point URL
 - https://wt-cmrp-100.wolftech.ad.ncsu.edu/reports
 - Users should expect to have their consoles upgraded on next sign-in. Likely you have already experienced this for this upgrade.
 - State Migration Point removed this morning: https://sysnews.ncsu.edu/news/588768cc
- Current state of Kaspersky Migration (Michael)
 - A stand-alone installer has been provided here:
 - https://software.ncsu.edu/faculty-staff-university/endpoint/
 - Currently ~8900 machines in the collection
 - Reminder we'll force the upgrade from Kaspersky to Endpoint Protection on February 17th 2017
- Have we done enough to prepare for the go-live of OIM? (Billy and Derek)
 - What are currently doing to protect AD from a bad OIM go-live?
 - Dumps a subset of AD attributes (everything OIM is supposed to be manipulating) to a CSV. (see details in Appendix 1 below)
 - Need to add GUID/SID
 - Nightly backups of DC's.
 - AD Recycle Bin (180 days).
 - When is the deadline of the OIM service account approval by the committees?
 - There are production groups that have appropriate permissions but haven't been validated recently.
- Setting up One-way Selective Auth Trusts with other UNC Schools (Billy)
 - 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 (Billy)
 - https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privile ged-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/
- Where should we deploy proxy .pac files from?
 - From Windows 8/8.1 and on you have to deploy .pac files from a web address.
 - Security and compliance has asked where they can/should put .pac files to support better tailored settings for proxy servers
 - OCSP If not used for PCI
 - Firewall baseline updated for new OCSP
 - There are currently 2 different .pac files for users to choose to use for datacenter resources
 - All NCSU IPs direct
 - If NCSU IP bypass proxy, internet goes through proxy
 - Only proxy for DUO service
 - Traffic to DUO goes through proxy, all other traffic "blocked"
 - DUO has the ability to set a proxy server for DUO authentication during client install
- Comtech changed DHCP Option 252 to null (https://sysnews.ncsu.edu/news/58861644)
 - If you see anything unexpected please speak up
 - This goes toward the killing of WPAD
 - Are there other things we can do to take a proactive approach
 - Set the Auto-Detect for INET1 at a higher level (NCSU Policy)?
 - Issue would be that this setting is a User Configuration setting
 - Auto-Detect Off
- Billy: It's unclear whether Macs in AD support pre-auth. It is not set in userAccountControl by default and there are seemingly a lot of pre-auth errors in the DC logs.
 - https://blogs.msdn.microsoft.com/muaddib/2013/10/28/how-to-find-user-accounts
 -with-kerberos-preauthentication-disabled/

Appendix 1: (01/30/2017; ddballar)

Attributes dumped in nightly cron job for WolfTech AD user accounts in the /People OU. Most of these are editable, a couple of them are for reference only.

- "sAMAccountName"
- "userPrincipalName"
- "ncsuCampusID"
- "GivenName"
- "middleName"
- "sn"
- "initials"
- "displayName"
- "mail"
- "uidNumber"
- "gidNumber"
- "loginShell"
- "ncsuAFSPath"
- "userAccountControl"
- "gecos"
- "px"
- "lastpasswordchangedate"
- "oimpasswordexpirationdate"
- "whenCreated"
- "whenChanged"
- "lastLogonTimestamp"
- "LastLogonDate"
- "Enabled"
- "objectGUID"