AD Policy Working Group
February 21th, 2014
3110 Engineering Building II
3pm-4:30pm

Voting Members: ~~Donna Barrett, Charles Cline~~, Dan Green, Julie Tilley, ~~Dan Evans~~, Daniel Henninger, Tom Farwig, Joshua Gira, Payman Damghani

Ex Officio Members: Alan Gerber, Michael Underwood, ~~Gene Morse~~

Guests: Billy Beaudoin, Debbie Carraway

Business handled outside of meetings:

- Raising WolfTech Forest/Domain Functional Level (12/18/13)

  We have a request from Derek Ballard to proceed with the upgrade of the WolfTech domain and forest functional levels. He would like to do this on Jan 2nd, 2014.

  - WolfTech current forest level: Windows Server 2008 R2.
    - We will move the forest level to Windows Server 2012.
  - WolfTech current domain level: Windows Server 2008 R2.
    - We will move the domain level to Windows Server 2012.

  The WolfTest domain was migrated back on November 4th without any issues.
  https://sysnews.ncsu.edu/news/5272b857

  The Windows Server 2012 forest functional level does not provide any new features, but it ensures that any new domain created in the forest will automatically operate at the Windows Server 2012 domain functional level. The Windows Server 2012 domain functional level does not provide other new features beyond KDC support for claims, compound authentication, and Kerberos armoring. For information on these new Kerberos options, see
  http://technet.microsoft.com/en-us/library/hh831747.aspx

  ACTION: Committee Approved 12/18/13 and requests that the Domain Admins proceed with the upgrade (and posting on Sysnews).

- XP End of Life Warnings on Wolftech AD (01/29/14)
  As discussed at the last AD Technical Committee, there is some concern that we're not being proactive enough regarding the number of XP objects remaining on the WolfTech domain. As of today, we have 1150.

We have proposed two approaches to address this:

1. Creation of a login message for all XP machines via Group Policy (limited to XP machines). Everytime someone logs in to a Windows XP computer, we want to display a warning message:

WARNING! This computer is running Windows XP, an operating system which will soon stop receiving security updates and patches. Effective April 30th, NC State University plans to remove these machines from the campus network. It is CRITICAL that you contact your local IT support to schedule an upgrade of this computer as soon as possible.

I'm open to suggestions with the wording of the message. Whenever the exceptions process is made available to us, we can create a mechanism to not display the message on those that get approved.

2. Weekly reports to OU Admins regarding the XP objects within their OU. Using ADToolKit, I can run a report (Computer Date Information) that provides a list of all computer objects in your OU and when they were created/last updated. I can also limit this to those with Windows XP as the operating system. Using the domain cron option, I can force this report on all OU Admins.

If AD Policy agrees, I will announce via SysNews/AD list explaining to everyone what to expect, then implement both.

ACTION: 2/4/14 -- Committee rejected proposal #1 and enthusiastically endorses proposal #2. Dan Green will setup the weekly reports to run Monday mornings and will announce via Sysnews / AD list.

=====

Agenda:

New Security Representative
Please welcome Payman Damghani as our new representative from Security & Compliance.

KANE/LONO Update (Dan G)
After many years, the KANE/LONO file servers which hosted all of the domain backups and GPO based software packages, have been retired. All of the former were moved to celerra over a year ago and the packages have joined them as of last week. All NCSU level packagers have been informed and provided access to the new fileshare.

IE9/IE10 Vulnerability (Dan G)

I sent an email to the AD list regarding this new vulnerability (http://www.computerworld.com/s/article/9246461/Microsoft_delivers_stopgap_defense_against_active_IE10_attacks?source=CTWNLE_nlt_dailyam_2014-02-20). Is there anything to discuss? Anyone who thinks we need to be more aggressive? Payman will consult and get back with us.

Trend AV Discussion Update (Tom/Michael)
There's been a lot of discussion on the lists over the past couple weeks about the status of the Trend AV SP3 package causing reboots. Has a conclusion/solution been found?
The packages have been updated to no longer constantly reinstall. Either SP2 or SP3 package will result in a current version installed. No reason to move computers from SP2 to SP3 (as they'll already have been updated by the service. When we get ready to move to Kapersky, that installation will clean off Trend as a part of its installation process.

ACTION ITEM: Explain this to the OU Admins in a simple email

2012 R2 Domain Controller Upgrades (Billy)
Being done in March (Spring Break) and as a part of this will also move them behind the newer ASA firewalls that ComTech now has in production. Closes out one of the AD Audit findings. Will also help with the firewall auditing requirements of the audits discussed below.

PCI and Financial Systems Audits (Billy/Debbie)
We've just begun the discussions on what will need to be done to the domain so it can pass upcoming PCI certification and State of NC Financial (based on ISO 27002) systems audits.

Windows 8.1 Baselines (Dan)
We've been struggling to find the time to review the Windows 8 and Windows 8.1 baselines and release them to the domain. While we still need to do so, I'd like to propose that we release an initial Windows 8.1 baseline using the official MS Windows 8 baselines in the short term so we have *something*. I'd further recommend that we enable the policy that allows Windows 8.1 to pull its .Net updates from Windows Update rather than the default of trying to talk to the WSUS servers and failing (we've already pushed this for Windows 8 machines).

ACTION ITEM: Committee requests that AD Domain Admins update the current baselines for Win8 to use the Win8.x WMI filter, pushing these policies to 8.1 as well as 8.0. We still need to fix the policies.

MS Dreamspark (Josh)
Josh informs us that MS had told Bill Coker that a University level license for Microsoft Dreamspark is not going to be possible. Individual college and departments can continue to register on their own and should consult with Bill as he now has a code to allow free registrations.