

WNAG

Meeting: 2017-09-20

Present: Jim Johnston (Chair), Anton Romantsov (Secretary), Lowell Williamson, Bernie Rutter, Allan Fleming, Clayton Tucker, Nevil Bromley, Ray White, David Aldwinckle, Mike Patterson

Previous Business

Chorus domain:

Engineering continue working on dhcp, DNS. Labs converted to Chorus (workstations joined to the new domain). Users login with Nexus accounts.

Certain machines had communication issues with Nexus DCs, fixed after reboot. Could be a workstation issue as well.

Issue with samba: lost indexes, reason unknown. IST is tracking this here:

<https://rt.uwaterloo.ca/Ticket/Display.html?id=646988>.

Ecfile1 overloaded, ran out of memory. Shutdown the server and re-joined the domain to fix. Moved ECfile1 to the correct OU.

Comment from wnag: suggest submitting an update in advance

New Business

Users in NEXUS which are not in WatIAM:

A number of compromised Nexus user accounts not controlled by WatIAM. These are old accounts in legacy groups, mostly in Engineering OU, passwords last reset in 2001 and still valid.

Mike will submit a breakdown list of users to faculty reps.

Ldap service certificates renewal on Nexus DCs:

GlobalSign CA no longer permits renewals of publicly trusted SSL certificates (Organizational type) that are used to secure internal server names, reserved IP addresses & domain names. This affects any certificate on a server with IP address in a private subnet (172.16.x.x), including LDAPS certificates on Nexus DCs. The certs on the first four DCs will expire on November 13-16, 2017, the fifth in December 2017 and the last in February 2018. As these certificates can no longer be renewed as Organizational, IST is planning to renew them as IntranetSSL certificates.

Dave A will investigate if we can change ldaps farm configuration to terminate initial client connection at the F5 and from F5 connect to a DC as plain text.

DCs upgrades:

Moving to new hardware and new OS (Server 2016). Test environment already upgraded to 2016. We're thinking to start upgrading DCs in Prod within next couple of month if no issues. We're not planning to raise domain/forest functional levels at this point.

New features supported in Server 2016 ADDS:

1. Privileged access management (PAM)

2. Azure AD Join
3. Microsoft Passport

Faculty Updates

(Agenda items submitted)

AHS – Lowell

BMH 2nd Floor renovations are continuing
Mobile lab (cart and ~20 laptops)
Built and now a bookable resource
2nd Lab of MS Surfaces in place (issues with hardware)
Planning to implement UEV
Migration of applicable 2012 servers to 2016 - ongoing
Issues with 0365 accounts not being activated or compromised

Arts – Nevil

Accounting Lab moved to Win 10
Looking at class lists with Grouper
Learnlock working with Win 10, some intermittent issues

Computer Science - Clayton

Clayton Tucker replaces Steve Nickerson as CS representative.

IST – Manfred

- We plan to block NTLMv1 to our Netapp starting October 10th. We have a handful of workstations still connecting using this protocol. Ones that are left in the faculties (today) include:

magneto 129.97.127.180 NTLMv1 NEXUS\m2gaspic SMB2_1 (Science)
magneto 129.97.185.83 NTLMv1 NEXUS\rmpringl SMB2_1 (Arts)
magneto 129.97.250.58 NTLMv1 NEXUS\mhturhan SMB3_1 (Eng/Mech)
magneto 129.97.40.207 NTLMv1 NEXUS\jnvanwyk SMB2_1 (Eng/Chem)
magneto 129.97.47.12 NTLMv1 NEXUS\oakley SMB3_1 (Science)

- We have too many users contacting us from Eng and Math, saying they can't get MS Office or Windows 10 activated. Is there a reason they are not all using campus DNS (or not in Nexus)?

- Trying to reduce the number of Nexus computers to "managed" (only) and migrate the remaining "client managed" ones.

- We feel there may be a place for computers in Nexus that have the bare minimum of mostly security-related GPOs applied. This group would consist of mostly PCs that rarely appear on campus after the initial build (but are still UW-owned). This way they at least get configured properly once, and get updated when they do reappear, either on-campus (or via VPN when we get that far). This local "Nexus" logon is cached and would provide clients some advantages of already having authenticated when they reach across to campus resources.

- Starting to have Client Services block Chrome settings from UEV, because of growing size issues. Options are being investigated.

- Are discussing details of how to best get AS clients from the W10 "Evaluate" phase/ring to "Pilot" to "Broad", where "Evaluate" is about 7-14 days (5-or-so clients), "Pilot" is about 1-2

months (200 clients expected/hoped for), and “Broad” deadline is yet to be determined (all remaining clients).

Math – Jim

More Windows 10 upgrades in offices.

Nexus PCs had problems registering with KMS server (licsrv3)

Comments from w nag:

The NTLMv1 change didn't raise an alert with anyone.

On the KMS licserve3 topic, there was a problem with firewall blocking access. Manfred's team made changes that should help alleviate Windows10/Office2016 activation issues.

Other Business

Arts, Science, Math have new student accounts who didn't get the N drive created. Most likely a result of a configuration issue with a script that adds home folders for new users. The issue with the script was fixed in July. New user accounts opened by WatIAM after that should get the home folder created automatically. However, adding the folder manually may still be required for accounts opened before the problem was fixed.

Changes are coming to the way how mobile labs join eduroam. Dave A will provide more details later.

Arts, Math: class lists data in grouper still missing. There is a work in progress.