MINUTES

WNAG

Meeting: 2015-08-19
Present: Arts - Nevil Bromley; ENG - Steph Sempson, Ray White; IST - Manfred Griesbach, Dave Hinton, Ravindri Kutulnaga, Will Lewis, Mike Patterson (Secretary), Anton Romantsov; Math - Hari Chotara; Science - Allan Fleming.

1 Previous Business

1. Unlinked GPOs (Dave): ENG asked if these were really causing issues. Dave says that yes, they are — Microsoft has said that this is a problem both during troubleshooting and an AD audit. Is it causing actual performance or other issues? Not provably, but apparently ours is sufficiently deviant that Microsoft had to rewrite some of their auditing tools to account for us. Chair requested a fixed timeframe for a cleanup, suggested 3 months. There was no great disagreement.
2. DC migration to private subnets - update (Dave): All happening this or next week. Upgrading certificates, moving last two to a private network, and patching them all. One patch is an LDAP rollup that will hopefully fix some issues we've been seeing.

2 Faculty Updates (round table)

AHS

- Working on lab rebuild using sccm
- 6 new workstations for SPHHS lab
- Migrated all software away from GPO to SCCM
- Interested about the support/documentation of:
  - Emerge
  - Appfilers
- Windows 10 test PCs have been deployed
- RLS Grads moving to uPrint
- Investigation of new SAS deployment `http://www.sas.com/en_us/software/university-edition.html#m=get-free-software`
- TechTown moves of research groups has been time consuming

Math

- Upgrading one of the undergrad labs with new thin clients. We are deploying Windows 7 based thin clients instead of ThinPro based.
- Retired 2 oldest undergrad terminal servers, added one new terminal server. Now, all undergrad terminal servers have 10G connectivity. We are using NLB and RD Session Broker for connection and load balancing. NLB with multicast setting didnt work with our Dell network blades as they wouldnt allow ARP entry with unicast IP address and multicast MAC address. So, we used 2 network adapters in place of single and configured unicast NLB which works better.
- Upgrading common apps. We will be using SCCM for common apps instead of GPO which we used till now.

IST-ISS

- Ended zip file embargo on Connect as of 1530h, 18 August.
- re last month's minutes: currently have no plans to expand Globalsign contract beyond the current year to year, which is what would be required to issue "free" certificates with lengths > 1 year.

3 New Business

1. AD query return limit: Steph Sempson spoke to the request to up the query limit so he can more easily populate such groups as "all Engineering undergrad students." There was much discussion, but he would like to have a limit of 20,000 to accommodate that particular request, plus have a bit of headroom, and thinks any resulting performance issue is unlikely. From a security point of view (Mike) there's no difference between allowing the current limit or 20k — we know people are scraping our directories and the only way to stop the scraping is to detect it while it's happening and disable access, not to put in a limit. DaveH: a separate RO DC will not help (may make it worse). Anton's concern is there is currently an open case with Microsoft related to LDAP and he doesn't want them to point to this as an issue. Eventually tabled: "can we live with making the change as Dave suggested, provided Steph understands that things might go away on very short notice if Anton requires?" No abstensions, no disagreements. Dave's suggestion was to raise the limits permanently with the understanding that *if* dropping them is required, it might be done on very short/no notice.
2. New chair and secretary: Nevil's 2 years is up shortly. Mike's 6 months is also technically up, but he will take minutes for another six months. Preference for chair would be non-IST staff, as this is intended to be primarily a faculty group.
3. Password implementation in IST (Manfred): LAPS allows us to programatically change local admin password on a PC. Being implemented on workstations in AS. MS tool has been available for years, but only to Premier customers, now it's free. Made schema change: added two attributes. DIT did not increase in size. A group policy extension needs to be applied to workstations for this. AS had it pushed by SCCM; actual control is by OU, and control is delegated to OU admins. Password is stored in an attribute plaintext, who can see that attribute can be controlled. Minimum of 16 characters, random alphanumeric. We could even do daily changes if we want. Tested on 22 IST PCs, will roll it out to the rest of IST shortly. What happens to PCs that are offline for a significant amount of time? The password won't be changed if it's not online (convo between AD and the workstation).
4. Sharepoint GPO (Manfred): Stephen Markan and Jenn Matheson suggested that we add Sharepoint names to the local intranet group on workstations. Manfred requests that people try it out and see if

it's suitable for being added to all endpoints. Eng and Arts already use these settings — what Manfred suggests should not replace what might be already there. Manfred suggests we wait for Nevil to finish the testing he wanted to do, then send out a change request. (What OU is it done at? Manfred thinks People. Ray thinks they do things through machine OUs.)

4 Stalled Items

1. LDAP requests requiring a trusted source (Dave): let's remove this from the agenda for now. So many applications don't use ldaps. :(

2. GPO to log successful logons (Dave): well on our way to having this complete, or it is already complete, so remove this too.

5 Other Business

1. AD consolidation: majority now deleted. This has caused pain for some who were not paying attention.

2. Emerge question (Lowell): who is responsible, where's the documentation? Paul Dietrich and David Canzi are possibly the people working on it. Version is marked 1.0, but there's a 1.3 release. 1.1 was for a non-Windows OS, 1.2 was for a different, and 1.3 might be a 32/64 bit package. Lowell observes that since this is about safety, it needs to have regular attention. Dave will look into this (and could talk to Jason Testart/Dan Anderson) and see who needs to own this service. Ray observes that the client is extensible and you can have multiple servers talking to the client. For example: Chemical could have their own server so that they can push out more localised notifications (eg, a leak in E6). Ray's not sure if anybody is actually making use of this functionality.

3. VDI/Access licensing (Nevil): How does it work? Staff members can RDP to a workstation in order to gain access to these things, but students cannot, unless they have it installed locally. Or if students are using university-owned equipment to RDP to a terminal server, they're covered.

4. Windows 10 licensing: it's complicated. Ask Manfred. Migrating Win7 Ent $\rightarrow$ Win10 Edu loses applications.