Agenda

WNAG

June 21, 2017 9:30 – 11:00 EC2-111

Previous Business	
R/O Domain Controller	Ray/Dave

New Business	
SharePoint GPO	Jim

Stalled Items
None

Standing Items	
None	.

Faculty Updates

AHS – Lowell

- BMH 2nd Floor renovations have begun (behind schedule)
- Planning for a mobile lab (cart and ~20 laptops)
- Cart ordered and laptops have been selected
- Lab rebuilds to take place in late August
- Planning to implement UEV
- Setup management server to monitor events (FrameFlow)
- Migration of applicable 2012 servers to 2016

Arts – Nevil

- Lab rebuild for ML113 change from 25 stations to 16 laptops on Nexus
- Renison moving towards SCCM
- EUFI boot and SCCM issues
- Last lab HH280 scheduled to be upgraded to Windows 10 in August.

Agenda

Computer Science - Steve

- Nothing to report.

Engineering – Ray

- No report submitted.

Environment – Bernie

- Preparing for multi-week full power outage in EV1 (August 7 - ??)
- ENV WSUS Pilot continues
- Getting Windows 10 machines up to date

IST – Dave/Anton

- Nothing to report.

IST – Manfred

- We discovered the "BUILTIN\Administrators" group needs to be added to the "Access this computer from the network" policy (explicitly) for W10 administrators to be able to RDP into the PC. (With W7 this happened implicitly.) We do this now by GPO.
- We now disable the "Windows master browser service" by GPO on all of our workstations since we have noticed that turning it off in the deployed image was being undone by updates, and some workstations were latching onto others (instead of DCs) as their master browser.
- UEFI support now exists within the IST W10 image. If the BIOS of the laptop is configured to UEFI, that image, with the required additional disk partitions will be deployed. If the BIOS is configured to legacy mode, the image we've deployed up until now will be deployed.
- We now have a "Shared Access Workstations" sub-OU under IST (like the "Public Access" one in many faculties) that we put breakout room and boardroom/meeting room PCs into. (Any PC that is typically used by more than one person.) Then we apply the newest "Clean" utility we run on all Podium PCs to them. It deletes local profiles, removes temp files and reboots each night. It also (optionally) runs defrag and backs up event logs, if needed.
- Laptop W10 deployments in AS were failing on occasion, and investigation showed that they were docked at the time. We do not currently have (nor can we keep up with) all docking station NIC drivers in PXE or in our OS images, so to avoid the problem, we are now asking clients to plug the Ethernet jack directly into the laptop for the imaging process (and change it back to the docking station when done). For laptops without an Ethernet port, we plan on recommending a limited number of adapters, and a limited number of docking stations for future purchase.
- MBAM clients may start rolling out soon, along with Bitlocker and MBAM GPOs. It's important to know that MBAM GPOs will manage the Bitlocker GPOs, so any existing ones (we don't have any in AS) may be modified.
- MBAM has been helpful already in recovering keys, but still has a problem kicking off an encryption without explicitly being told to do so. We're still working on it. (It will encrypt just fine but not automatically when the client is installed (if that is the configuration))
- We're still working on developing a plan to properly manage and vanguard W10 CB versus CBB rings on behalf of our clients. This has been complicated by the fact that Microsoft offers several versions of W10 as CBB, and a new CB version is expected in September.

Agenda

IST - Ravindri

- Nothing to report.

IST – Security - Mike

- This past week, we've noticed 2 malware infections. Same symptoms, two different OUs (AS, CS). We see a JS downloader, followed by Andromeda. In two cases, Andromeda was followed by Pony. In one case, the machine was left online longer (thanks, weekend) and wound up emitting spam / malware emails. We don't know how these got onto systems. My presumption is that these were drive-by downloads, but investigation is ongoing, and we often are unable to come to a conclusion anyway. Unfortunately the AS machine just got re-imaged and pressed back into service. CS has used a couple of tools to try to eradicate, but they're not working.

  I only mention this because since Proofpoint came into play, malware infections have been way down: since Aug 2015 or so, almost all malware infections we could attribute were from email delivery, a switch from the prior trend of driveby downloads. I don't know if the CS user is also an Exchange user, but the AS user definitely was. It's possible we might see a shift back to drivebys, which would be unfortunate as I was hoping for another year of relative peace...

Math – Jim

- Started Windows 10 upgrades in offices.
- Found a solution for problem where SharePoint keeps prompting for a password. In IST-RT#572418 Math proposes that IST changes "AS – SharePoint" GPO per instructions in:

  https://blogs.technet.microsoft.com/office_integration__sharepoint/2014/02/24/prompted-for-username-and-password-when-opening-an-office-file-from-a-web-server

  Effectively, "**HKLM\System\CurrentControlSet\Services\WebClient\Parameters"** needs https://*.uwaterloo.ca smb://sharepoint.uwaterloo.ca

Other Business

?

- ?

Additional Notes

Regrets: Allan