MINUTES

WNAG

May 20, 2015

Present

Nevil Bromley, Arts (Chair)	Hari Chotra, Match
Ray White, ENG	
Manfred Grisebach, IST	
Will Lewis, IST	
Bernie Rutter, ENV	
Ravindri Kulatunga, IST	

Regrets

Lowell Williamson, AHS

Dave Hinton, IST

Mike Patterson, IST

Previous Business

Faculty and Dept contacts

Engineering provided a list. Full list to be posted on WNAG sharepoint https://sharepoint.uwaterloo.ca/sites/wnag/_layouts/15/start.aspx#/Shared%20Documents/Forms/AllItems.aspx and http://windows.uwaterloo.ca/Faculty_Contacts.htm

IWAG update

IST has been encountering issues with machines being turned off during scheduled windows updates and are investigating / implementing scheduled reboots of workstations in Academic Support.

Windows Operating systems and campus licensing were discussed regarding what will happen once Windows 10 arrives. IST expects the campus and industry will continue using Windows 7 until at least Windows 10 SP1.

New Business

Reminder to report malware incidents.

Members are reminded to submit reports of successful and partially successful malware attacks to soc@uwaterloo.ca. An example of a successful malware attack is one where the user reports difficulty using their PC, and investigation determines malware to be the cause. A partially successful attack is where antivirus reports that it blocked malware *after it started running* - ransomware encrypts a few files before being deleted, for instance. If in doubt, please report. These reports assist SOC in coordinating response and looking for other infected machines that have yet to be reported. Members should please pass this along to IT co-workers who are not in WNAG.

OU containers and objects

The existence of security groups in the people OU was discussed.

Windows Firewall

Windows Firewall has been misconfigured on campus for some time now, since we all seem to have carried on what was set up in WXP. (SEP in our case also used WF, so probably still good to redo, as spelled out below.) One of the better docs on setting up WF via GPO can be viewed at: http://www.grouppolicy.biz/2010/07/how-to-manage-windows-firewall-settings-using-group-policy/
There it says:
"If you have already configured firewall setting under the older "Windows Firewall" section these policy rule will also apply and the two rule sets will try to merge with unpredictable results. I recommend that you make sure that no "Windows Firewall" setting are applied to your Vista/2008 or greater computers and that you solely apply the firewall setting to these newer computers via the "Windows Firewall with Advanced Security" group policy security option."
So I did some testing.
Sure enough, when you look at WF Advanced settings on any W7 PC, and apply older WF rules via GPO, many new rules get added to the existing list, most/all? of which mirror settings already there, but they are worded differently. NOTE: And this is significant: New rules did NOT get touched, so conflicting rules are possible. . (Is this why we have problems sometimes?)

When a new GPO was configured leveraging only Advanced WF (AWF) rules in IST, 28 old rules disappeared again, which is good. So far I have been able to configure all settings (but 2) via AWF, and are in the process of testing before removing old rules from all of Academic Support. (The final 2 may not be needed.)

BTW: I know we discussed export and import but have not tested this as it was quick to manually define advanced rules. Also, I needed to be sure "old" rules did not get imported if this was done. By not importing, I'm sure.

Standing Items

AD Consolidation Update

ADS still present

Unlinked GPO

Seems to be better.

Round Table

IST Manfred

- Starting to gear up for W10 and Office 2016 – Microsoft giving W10 presentation June 10th @10am in MC2009. (Not planning on mass deployment until at least SP1, but are planning to go there ASAP.)
- Launching a tool to force weekly reboots on all AS managed PCs – Changing how we deploy patches, etc.
- Beginning to modify BIOS on PCs to power up for management @2am. Too many problems with clients affected if PC not left on when required.
- Workstation Services and rest of ITMS, minus equipment loans, moving to EC2 end of May
- Looking @BitDefender and Kapersky as possible EP solutions for our 400 Windows servers
- Opened up Windows Firewall to include "File + Printer Sharing", ICMP and WinRM for all AS computers. Removing SEP closed some of these doors so needed to open again.
- SAS is free now (in the "cloud"), so may reduce migration to VDI requirements
- Have over 3000 workstations running SCEP now (1400 in faculties last count)
    - Will be introducing executable for SCEP @home shortly

    - Not licensed to run Security Essentials on UW-owned W7 home PCs
    - W8 comes with Defender, so already done
- Managing local Admin access on PCs in AS via SCCM

IST – Security Mike

- Conference

Engineering

-

Math

- Migration to new netapp encountered some difficulties

Arts

- SCEP deployed to all Arts machines
- Psych investigating SCEP
- **Ongoing SCCM implementation and automation**

ENV

-

AHS

- **AHS workstations are migrated over to SCEP**
- **servers still on SEP**
- **Working on images for the fall term**
- **SCCM development continues**
- **Labs hardware to be replaced during summer term**

CS

-

Science

-