IOWA STATE UNIVERSITY
IT Services Technical Notes

IT

Windows Administrators Meeting

January 14, 2011
Notes (taken by Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- **Domain policy change January 4, 2011 (roaming profiles)**: The Enterprise default domain policy was changed January 4, 2011 to disable roaming profiles except where explicitly allowed by local or group policy. See the following for complete details: http://www.tech.its.iastate.edu/windows/admin/Announce.2011.01.04.pdf
- **Fax number on user objects:** The fax number is now being synchronized from enterprise master sources into the Active Directory user object (on the "Telephones" tab in the "Fax" field). The fax number is mastered by Human Resources and can be changed via AccessPlus (select the "Employee" tab and look for "Address Change" in the menu). Since the AD fax number is now mastered from official university sources, any changes manually done by an OU administrator will now be resynched (erased) and replaced with the official university data. This is the same as other important user attributes. See point 5 in the section "Managing ISU NetID User Objects" in the following TechNote: http://www.tech.its.iastate.edu/windows/admin/UserMgmtInOUs.pdf
  A synch operation has already been performed, meaning that if you have a fax number on AccessPlus it is now present on your AD user object.
- **New Institutional Lists/Groups:** The college/major lists have been divided into three new lists. For example, the "engr_coll_ugrad" group is now composed of three groups – past_engr_coll_ugrad (graduated students), current_engr_coll_ugrad (current students), and future_engr_coll_ugrad (newly registered students). For more information see: http://www.tech.its.iastate.edu/windows/admin/Announce.2011.01.09.pdf

Status Reports

- **CyFiles:** Steve Kunz [ITSYS] and Mike Lohrbach [ITSYS] indicated that ITS is very close to creating a 5 GB file space for each NetID-based user on an ITS NAS storage server. This is personal space for each user, which they have full rights to. Each time a new user registers for an account the space will automatically be created. In the near future (probably next week) a creation process will be run for all existing users in the domain. At that point every user will have an online folder (and full rights). ITS will be working with some colleges already using home folders to integrate this space as their home folders in AD. In the future "phase 2" of this project, this space will be integrated into every user object as the home folder and be automatically connected via a drive letter ("U", for example). The second phase of this project requires coordination, documentation, and training with all IT units, users, etc. The following questions were asked:
  1) Would the space be backed up? Yes.

2) Could the user initiate a restore themselves? Yes – right-click and select "restore previous versions"
3) Would there be a charge for a restore? Unknown – maybe, if it has to come from tape.

- **ASW mail-list -> AD Contacts:** Steve Kunz [ITSYS] said that this project is close to being in production. Final production testing should happen in the next week or two. For more details see "ASW Mail-lists as Contacts" in: http://www.tech.its.iastate.edu/windows/admin/WinAdmin.2010.11.12.pdf
- **PSOs (Password Setting Objects):** Steve Kunz [ITSYS] said that this project is off the back-burner and being worked on again. For more details see: http://www.tech.ait.iastate.edu/windows/admin/PSO_Planning.pdf
  This project has PCI-compliance (credit-card processing) implications and is scheduled for completion by spring 2011.
- **Secunia CSI:** Mike Lohrbach [ITSYS] said that the Secunia CSI server project is nearing completion. Secunia CSI is a "system update" system much like "Windows Update" that checks for much more than updates to Microsoft software. Secunia will check for Java, Adobe, and many other popular third-party software products and find out of date versions and provide a means to upgrade the software. The ISU licensed product will integrate with the existing SCCM and WSUS update systems. See www.secunia.com for more information on the CSI (corporate licensed) and PSI (freeware for personal use) software products.

Watch for further announcements for all these projects in the CCSG and WinAdmin groups. Send any feedback/comments to the person tagged on the topic (Kunz or Lohrbach).

Security – Campus Border Block Proposals - RDP [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] said ITS is still moving toward blocking Windows Remote Desktop Protocol (RDP, port 3389) at the campus border. This item was last discussed at the October 2010 WinAdmin meeting:
http://www.tech.its.iastate.edu/windows/admin/WinAdmin.2010.10.08.pdf
ITS has extended the proposal to include SSH remote terminal (port 22). These steps are needed considering the large number of probes/hacks using these protocols from off-campus. When such port blocks are implemented there would be three main ways to get into campus:

1) Use the Cisco VPN server (and an AnyConnect VPN client)
2) Use a different port number other than 3389 (RDP) or 22 (SSH)
3) (If 1 or 2 are not possible) Request an exception for the block through the ITS Security Group

Steve Heideman [CHEM] asked what could be done if software vendors used RDP to access systems on campus for maintenance.

Send any feedback to this project to Wayne Hauber [ITSEC] at wjhauber@iastate.edu

Security – Campus Border Block Proposals – mailhub [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] outlined changes to the mailhub system needed to prevent "mail blacklisting" of Iowa State University email systems. Kent Ziebell [ITSYS] found on December 18, 2010, that off-campus email spammers had discovered a technique to circumvent our obfuscated security on our main SMTP mail transport system "mailhub.iastate.edu" (the technique will not be detailed here for obvious reasons). As a result, most ISU email systems were "blacklisted" to prevent transport of email from "iastate.edu" at many major sites off campus. As a result, ITS has developed a three step plan to secure the mailhub transport system.

First, on January 5, 2011 a new set of mailhub systems was created for exclusive use by the ITS Microsoft Exchange email system. The new "Exchange-only" mailhub hosts are accessible only by the ITS Exchange system and not exposed to off-campus usage/attacks. This immediately protects the ITS Exchange system from blacklisting by off-campus spammers.

Second, a new system of mailhub systems was created that require authenticated connections to send mail ("authenticated send"). These systems are available now and are not (and will not) be blocked at the border. Many mail clients such as Outlook Express, Eudora Pro, Thunderbird, Mac Mail, etc. can be configured to use authenticated sends. The Solution Center has prepared documentation on how to configure common email clients to use these servers. Go to http://www.it.iastate.edu/ and search for "mailauth" for more information.

Third, the existing mailhub system (mailhub.iastate.edu) will be blocked at the campus border (no date has been set yet). This means that any client attempting to send email through it must use a VPN connection to connect "on campus" first. Note that this means that any ON CAMPUS system will not be affected by the border-block (so servers or client systems that never leave campus have no changes). While no date has been set for the border-block of this system, should outside attacks ramp up again a block may need to be quickly implemented.

Contact the Solution Center for any client configuration questions you may have. If you have any feedback/questions on the overall architecture of the ITS mail system you can send it to Kent Ziebell [ITSYS] at ziebell@iastate.edu (no system configuration or usage questions please – use the Solution Center for that)

Security – TDSS malware [Steve Kunz on behalf of Wayne Hauber - ITSEC]

Steve Kunz [ITSYS] spoke about a topic Wayne Hauber [ITSEC] has been dealing with regarding the latest generation of malware being seen on campus. TDSS is a very well written piece of malware that cannot be detected or eradicated using AntiVirus software from any vendor. A system is usually infected by clicking an email link or drive-by browsing. A hidden file system is created on a system disk. Financial information and key-loggers are likely payloads. Once infected the only way a system can be cleaned is with a low-level disk erase (such Derik's Boot and Nuke - DBAN – www.dban.org) and complete rebuild.

The main point to be taken is the old "I have current DATs for my anti-virus software and scanned my system and it is clean" statement is not longer valid. Simply re-installing the OS from disks (with a delete and reformat the drive using the Windows install disk) is also not good enough, either.

Contact Wayne Hauber [ITSEC] at wjhauber@iastate.edu for more information.

Security – AntiVirus software [Mike Lohrbach - ITSYS]

Mike Lohrbach [ITSYS] talked about the very real possibility that ITS will not renew the site-license for McAfee AntiVirus on July 1, 2011. We are currently running under a one year extension of our license until June 30, 2011. This has become very expensive software and ITS already has licenses for Microsoft ForeFront (the Microsoft antivirus product) under the September 2010 purchase of Microsoft's "eCAL suite". Microsoft ForeFront can be managed individually on each system, via GPO (for OU management, via SCCM, and via a new "SCOM Server Management" system (for servers).

The dropping of the McAfee license (and promotion of Microsoft ForeFront) will have several implications:

1) There are no Microsoft ForeFront clients for Macintosh or Linux systems (it is "Windows only").
2) Students and off-campus personal use would not be covered by the Microsoft ForeFront license (the license covers "university-owned systems" only). People would have to convert to "Microsoft Essentials" (the Microsoft free package) or another free AV package (such as AVG).
3) Legal ramifications may be that all existing copies of McAfee AntiVirus must be removed by July 1, 2011.

Look for a survey to be presented to the CCSG group regard what anti-virus software you currently use and what implications the dropping of the McAfee license will have for you. Please respond to that survey!

The question was asked as to whether this would affect the McAfee AV license on the Exchange system. The answer was "No, that is a different contract".

Contact Mike Lohrbach [ITSYS] at mlbach@iastate.edu for more information.

Open Discussion

There was no time for open discussion.

Meeting Adjourned (10:00)

Next meeting is scheduled for February 11 (provided a sufficient agenda exists).