# Windows Administrators Meeting

July 9, 2010
Notes (taken by Steve Kunz)

## Meeting Started (9:00)

## Announcements

- On July 5 (the Monday holiday) WINS-1 had problems caused by the corruption of the WINS database. One of the ITS staff (Beata Pruski - ITSYS) noticed this from home and attempted to recover the database via a reboot and (when that didn't solve the problem) a restore from an online backup. All proper procedures were followed but the WINS database proved non-recoverable. In this case the only option was to delete the WINS database on WINS-1 and allow it to be rebuilt (by systems re-registering their WINS information). The hope was that replication from WINS-2 would work well enough to recover most WINS entries on WINS-1, but WINS replication has never worked very well and this appeared to be the case this time. On Tuesday, July 6 we sent out information to the CCSG and WinAdmin groups (and informed the Solution Center) that people may need to force a re-registration of their systems in WINS. For Windows, this is a "nbtstat –RR" command (if that does not work, a reboot).
- John Hascall [ITSYS] announced that "Wake on LAN" is available. Using "Wake on LAN" you can power down a system and have the ability to power it back up remotely using a "wakeup signal". Typically, you must enable Wake-on-LAN on the computer before it will work. For Windows computers, this generally involves a BIOS setting as well as enabling the option on the Ethernet Network Interface in the Control Panel. Once you have done that (see your system documentation), you can now send "wakeup" calls for systems you manage via ASW (http://asw.iastate.edu ). There are two methods of doing this. First, use the "Campus IT Admin Functions->Administer NetReg->Send Wake-on-LAN wakeup" and supply the hostname/IP. Second, you can use the "Manage user <netid>" ->Manage <netid>'s computers->View computers NetRegistered to <netid>" and click on the "wakeup icon" to the right of the hostname. It is important to note the if you shut down a system and then move it to a different subnet a subsequent wakeup call will not work (it will be sent to where the system was last seen on the network). The question was asked if there was a provision to wake up a range of machines (such as a lab). John's answer was "No", but it seemed like a good idea. Perhaps in version 2.

## Thawte Digital Cert Issues (Post 6/27/10) [Steve Kunz - ITSYS]

Steve Kunz and Bill Frazier [ITSYS] reminded everyone that on June 27, 2010 Thawte changed their digital certificates. They did two things: Create longer keys (from 1024 to 2048 bit) and segregated their "true root" (following best practices and/or mandatory procedures PKI). This CAN cause problems for any new certs installed after June 27. Make sure you follow the guidelines provided by Thawte (and not your old documented procedures) for the immediate future. You will probably have to install an "intermediate root certificate" from Thawte until all the updated root certificates have been pushed out to Windows (via Microsoft Update) and RedHat (via RPMs). You know you need to do something different for an SSL certificate, for example, when you see the error that says the connection is untrusted even though you have a current SSL cert.

### New ITS Directions on Bang-Accounts [Kunz, Lohrbach, Hascall - ITSYS]

Steve Kunz (with help from Mike Lohrbach and John Hascall) [all are ITSYS] discussed possible changes to the Windows AD bang-account support. Bang-accounts came into being during the Active Directory design process in 2000. They fill a need that IT managers expressed for the ability to provision user accounts themselves (sometimes on weekends or other off-hours) and have them "permanent" and managed by them. Currently the AD domain has approximately 4,500 bang-accounts (9% of the total number of user accounts).

ITS would like to move away from providing central services (such as Exchange mail) to bang-accounts but still allow bang-accounts to be created and used by departmental IT admins.

ITS has automation of the assignment of central services as a goal. One recent example is the automated creation of Exchange mailboxes for newly registered faculty/staff NetIDs (a process that used to be requested and provisioned manually). This is now done automatically for faculty/staff/affiliate accounts. This must be done manually for bang-accounts. Other services such as central online storage (NAS) cannot be used with bang-accounts because they do not have a unique GID (whereas centrally provisioned accounts do). As a result ITS intends to not tie central services to bang-accounts. For example, no services would be added to bang-accounts for:

- Exchange
- File service (NAS)
- Printing
- OCS
- ADIN

(There may be other services not listed above) Existing bang-accts will retain the services they have (so, for example, if you have a bang-account with an Exchange mailbox you will retain it).

ITS recognizes the need for special-needs accounts for services, visiting guests, and outside attendees for training, conferences, etc. If such accounts need ITS services we would like to see the replacement of bang-accts with affiliate/sponsored accounts. Sponsored accounts can have access to all services since there is ownership/responsibility inherited from the sponsor. ITS would encourage the migration of bang-accounts to affiliate/sponsored accounts.

ITS realizes there are some existing limitations on how affiliate/sponsored accounts are provisioned that may need to be changed. First, while the ASW web page allows for requests for such accounts, they are not automatically created at that time. The Solution Center staff must still act on the request to create the account. This may happen fairly quickly or it may take some time (depending on staffing, the hour of the day, or other issues). Second, you can only request one account at a time (so requesting thirty for a training session would be a pain). Finally, the affiliate/sponsored accounts suspend and expire after one year if they are not renewed (based on a yearly email to the account itself). To address these issues ITS proposes the following:

- Sponsored accounts be immediately available via ASW (no intermediate action required by staff)
- Multiple accounts can be created at the same time (with an incrementing suffix, for example)
- Accounts are non-expiring if used within past year
  - If idle one year, a warning email is first send to the sponsor
  - After <nn> days, the account is suspended
  - After <nn> days of suspension, they expire

The only people who would be able to create an affiliate/sponsored account would be faculty/staff. Students or affiliate/sponsored accounts could not create them.

There were several good questions about the proposed plan. What would happen to an affiliate/sponsored account when the sponsor leaves? The answer is that the accounted becomes flagged as “orphaned”. Currently the account would only be retained if somebody responded to the renewal email. Under the proposed plan the account would be retained as long as it is used (authenticated against). It was asked if the sponsorship of the account could be transferred to someone else. Yes, the Solution Center can do that now.

At this point ITS is looking for feedback on the proposed plan. You can send email to Steve Kunz [ITSYS, skunz@iastate.edu ] and he will forward it to other ITS members working on this proposal. This topic will be presented at an upcoming CCSG meeting for further public discussion. Let ITS know how this will impact your used of bang-accounts for the good or bad. If you have suggestions on how the current plan could be altered or extended to meet your needs don’t be afraid to offer them.

## Roaming Profile Support

Mike Lohrbach [ITSYS] talked about how the ITS storage committee is considering using the online storage on the NAS for user space, class space, etc. One possibility is to support Windows “roaming profiles”. Roaming profiles store various settings and user data (such as the desktop) on network storage and allow it to follow the user wherever they login to Windows. A few colleges (Engineering and VetMed) are already using roaming profiles for their own needs. The new ITS service could provide central support for all users. In addition, home folder and folder redirection could also be configured.

If implemented the roaming profiles would probably be an "opt-in" choice for the IT admins. Some IT admins already disable the use of roaming profiles on their systems (via policy) because of problems caused by profiles from other systems being dropped onto them. John Dickerson [ENGR] suggested we may want to look at a global policy change to disable roaming profiles by default (again, following an "opt-in" policy for those who wish to support them).

If you have any input into the roaming-profile/home-folders/redirected-folders discussion currently going on, send it to Mike Lohrbach [ITSYS] at mlbach@iastate.edu .

### Open Discussion

No time was available for open discussion.

### Meeting Adjourned (10:00)

Next meeting is scheduled for August 13 (provided a sufficient agenda exists).