Windows Administrators Meeting
January 25, 2002
Minutes (taken by Vince Oliver and Steve Kunz)

Meeting Started (9:05)

Announcements

- Jeff Balvanz (anti-virus software expert from AIT) has evaluated current anti-virus software in anticipation of the expiration of our NAI-suite (VirusScan, Virex, NetShield, etc) site-license. An "Anti-Virus Evaluation Open Forum" will be held Jan 29 at 2:00 in Durham 144). Email was sent out 01/24/02 to the WinAdmin group (and several other groups on campus) with instructions on how to get the evaluation report prepared by Jeff. This document is ISU INTERNAL ONLY (and should not be made available to off-campus/non-ISU readers). The email includes the link/username/password required to access the report.

Software Progress – Two-Way Password Synch

Kunz mentioned there is another delay on the two-way password synch project (where changes in Windows passwords will be reflected up to Acropolis for the ISU Net-ID). Other higher-priority projects have absorbed staff-time for the past week or two. This project should pick up again soon. Other aspects of Windows 2000 enterprise offerings depend on this "bottleneck".

Software Progress – "MountAFSHome" Command

Kunz talked about the "mountafshome" command, newly developed by AIT staff (Pruski). This command, when used in conjunction with the IBM/Transarc AFS client for Windows, will allow users to authenticate to the desktop, get AFS file access tokens, and mount the user's AFS home directory on a Windows drive at login time. The command works on Windows 2000, XP, and NT 4 (the same platforms supported by IBM/Transarc AFS). The syntax for the new command is:

mountafshome <username> <drive-letter> n|a

Where:	"<username>"	is the user's ISU Net-ID.
	"<drive-letter>"	is the drive-letter for the home-dir mount.
	"n" or "a"	indicates "no-append" or "append" to the C:\WINNT\afsdsbmt.ini file (most public-use systems will chose "n").

For "single authentication" to work (for access to the desktop and AFS-tokens) the AFS client must be configured to use the "Windows integrated login" feature. The username/password must be the same for logging into the desktop and getting the AFS tokens (always the case when your system is a member of the enterprise Windows 2000 domain).

The "mountafshome" command will be issued by a shortcut placed in the "All Users" startup folder with a command similar to the following:

mountafshome %username% H N

This will look up the current username's AFS home directory in Hesiod and mount it on drive "H". The mount will not be "persistent" (the next user logging in will not see it in the "AFS sub-mounts" list). Complete documentation on how to use the command will be included in the software kit when it is released. Three groups are now beta-testing this command. If you are

interested in testing you can contact Beata Pruski (bapruski@iastate.edu). [Aside: this command will also work on NT 4, but you need four contiguous free drive letters to achieve the mount, due to limitations in NT's mounting subsystem]

Software Progress – "pswdutil" Command

Kunz talked about a new "pswdutil" command he is developing. This command will allow OU administrators to enforce whatever password-age policy they wish on users in their OU. This is an alternate approach to the "domain wide forced password age" policy discussed in the past. Windows 2000 design has backed away from trying to force a single policy on the entire user community. This facility will let the various user communities choose their own policy.

The syntax for the new command is:

pswdutil –o <ou-path> [-u <username>] [-d <nnn>] [-t] [–q]

Where:	"-o <ou-path>"	indicates the OU to scan [Required].
	"-u <username>"	indicates a single username [Optional].
	"-d <nnn>"	indicates "find users with a password "nnn" days old or older" [Optional, defaults to "180"].
	"-t"	indicates "set" the flag to force the user to change their password at the next login.
	"-q"	indicates "quiet" (no output produced unless errors).

A new parameter of "-f <filename>" may be added to indicate a file where the command options may be supplied (so multiple operations could be performed with a single command). This command is intended to be run regularly by OU managers against their own OU (or sub-OUs within their OU). Users with different password-age needs could be grouped via OU, and this command run with different options for each OU. For example:

pswdutil –o "LAS/Chem/Users/Staff/Admins" –d 30 –t
pswdutil –o "LAS/Chem/Users/Staff" –d 90 –t

Here anyone in the "Admins" OU are forced to change their password every 30 days, but the remainder of the "Staff" only have to change their password every 90 days. Anyone in the "Users" container is free from being forced to change their password. Note that the "most restrictive" rule applies, if you are matched on multiple passes.

This software will be unavailable until the "Two-Way Password Synch" project is done (since users must be able to change their password in Windows once their "change password at next login" flag is set).

Student Organizations

Kunz outlined previous thinking about where "student organization" Windows 2000 OUs should go. It was first felt they should reside within the OU of their faculty advisor. Experience with the first couple cases indicated this was not the idea most departmental OU managers wanted to see. Student-run systems often have their administrators disappear over summer with no delegation of control to a new admin (mainly because they may not know who the person is for next fall). This means an upper-OU admin (or the enterprise admins) must manage the re-delegation of control. Current departmental admins (and the enterprise admins) did not want this task.

A design meeting was recently held with AIT User Services that resulted in a new approach. AIT User Services is already handling such functions for student-org web pages. Under the new approach, a "college level" OU (probably named "StuOrg") will be created with control delegated to AIT User Services staff. These staff members will deal with requests for OUs from official student organizations that have computer resources to be placed within an OU. The student-org OUs will have control of the OU delegated to the student admins (like any other OU) but the "escape-valve administration" (utilized in case OU admin-rights are "orphaned") will be handled by AIT Users Services staff.

Open Discussion

Kunz indicated if any existing OUs wanted to begin moving staff into their OU container it could be arranged. CIRAS (Chris Thach) has already done this. The only requirement is that your OU be repositioned/renamed to follow the standard naming convention (with official college/dept names).

Greg Wilson asked if people with ISU Net-IDs who have never changed their password would be migrated into Windows 2000 by some process. The answer is "no", since the password from the MIT Kerberos is unavailable, it cannot be synchronized during the move. The best approach is to still tell the users to "change their password" to be populated into the Windows enterprise structure.

FCS asked for an "Exchange 5.5 to Exchange 2000 migration status report". Kevin DeRoos (ADP, project manager for the Exchange 2000 project) indicated things were going well. Formal timeline is being worked on but not ready yet. He will be contacting the existing Exchange 5.5 admins about performing the first step (consolidating the Exchange 5.5 orgs into a single org).

Meeting Adjourned (about 9:50)

Next meeting Feb 8.