Windows Administrators Meeting
April 11, 2003
Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- A Windows Server 2003 2-day seminar is being offered thanks to Microsoft and a certified trainer. ADP and AIT are coordinating the effort of putting this on. We currently have enough attendees to hold the session (a minimum of 25 was required). We are working on booking a room more comfortable than Durham 144 for this size group. We will know more by end of next week. At that time people who emailed responses of "I would attend if offered" (to skunz@iastate.edu) will be emailed a link to a web page for formal registration from the certified trainer.

- Windows Admins are encouraged to test VirusScan 7.0 Enterprise Edition on both client and server systems (this product replaces existing NAI VirusScan and NetShield products). Kunz made two comments on differences people should be aware of. First, this product has an "On-Access Scan" feature enabled by default, which means any time a file is accessed by anything, a scan is done. This can cause a considerable slow-down in things like "volume de-fragmenting" or "Microsoft Office installations". It is easy to disable the "On-Access Scan" while such processes are running. Second, the new default action is to "scan all files". This is a change from the old "NetShield" product, where by default only files with certain extensions were scanned. There is a section in the "Readme.txt" file that covers this (check for the heading "SCAN ISSUES"). This section of the "Readme" states "For a comparable level of protection and performance compared to past versions, configure VirusScan Enterprise 7.0 to scan only "Default + additional file types".

Windows Enterprise Login Demo (Kunz)

Kunz is provided a demo of a small suite of products that provide a nicely integrated "single enterprise sign-on" to a Windows desktop that is a member of our domain.

The first component is a "replacement GINA" (a locally modified version of "BUGina" from Boston University) which changes the normal Windows logon/change-password graphics to "Iowa State University" graphics and can provide for departmental roaming profiles (or mandatory profile) support. Departmental graphics can also be easily substituted. The domain "drop-down" list is also hidden for the general user community (with text indicating "Supply your ISU NetID and password" for desktop login).

The second component is a "Kerberos V" authentication library replacement for the current "Kerberos IV" library. This is a complete replacement for the current

"C:\KERB" folder and contains core authentication routines used by Scout, PCLPR, PCAFS, Eudora Pro, WinZephyr, etc. The replacement library, combined with a new "Network Logon Service Provider" interface, provides both Kerberos IV and Kerberos V authentication tickets at the time the user logs in to the desktop. As a result, after getting the desktop no further authentication is required. Sidecar, for example, already shows being "logged in". When a person logs out (or the system is shut down) all authentication tickets are destroyed.

The third component is AFS file access. The Windows AFS client (available in the "Advanced" Scout-kit list) can be configured to use an "Integrated Login". In the "AFS Client Configuration" settings, on the "General" tab, check the box that indicates "Obtain AFS tokens when logging into Windows". If your system is a member of the enterprise domain, then the username/password to access the desktop will also get valid AFS tokens for file access to your files without further authentication. This feature, combined with AIT's "MountAFSHome" (also available in the "Advanced" Scout-kit list) gives the user easy access to their AFS home directory at each login. MountAFSHome automatically finds the AFS mount point for the user's home directory and maps it to a Windows drive letter. Since they already have credentials, they simply open files on the network-mounted drive.

The forth (and final) component demonstrated was the next version of "Hummingbird Telnet", which can use Kerberos V authentication. Kerberos V "pass through" authentication was demonstrated by opening a telnet connection to a "Vincent" UNIX system and having the existing Kerberos V credentials being used automatically to open an authenticated/encrypted connection. The next thing the user sees is a command prompt on the UNIX system. This "pass though" authentication will also work on Redhat Linux systems.

Several questions were asked about what combination of components were really needed to do certain things. Kunz stressed that the core component was the Kerberos V authentication library replacement (which handles all credentials at login time). The GINA component is probably only desirable in a "public use" environment where mandatory profiles (or departmental roaming profiles) are desired. AFS and Telnet components (both depending on the Kerberos V authentication library) are optional as desired.

The Kerberos authentication components will be distributed via Scout for the general user community by mid-summer. It is likely a "Lab Administrator" software kit will be prepared at the same time (for "summer lab builds"). The GINA is being tested by some departments right now and will probably be available as an "Advanced" Scout-Kit when fully tested. People willing to be "beta testers" should email skunz@iastate.edu to participate.

Open Discussion

Jim Wellman (AE EM) asked about distribution lists in the Active Directory Exchange 2000 environment. The question was whether or not you can add a "non-Enterprise-Active-Directory" mail address (such as "Yahoo" or "Hotmail" accounts) to an Exchange 2000 distribution list. Kevin DeRoos (ADP) replied "maybe". The Exchange 5.5 equivalent was a "Custom Recipient", which Exchange 2000 now refers to as "Local Contacts". These "Local Contacts" CAN be placed on a "Local Distribution List", but a "Local Contact" CANNOT be placed on an Active Directory Distribution List (so they will not appear in the GAL). Kevin also commented that other facilities are limited for such addresses. For example, scheduling a meeting results in only email being sent. Outlook calendar integration does not happen unless the person is an "Enterprise-Active-Directory" object.

Meeting Adjourned (about 9:45)

Next meeting is May 9.