Windows Administrators Meeting
July 12, 2002
Minutes (taken by Vince Oliver and Steve Kunz)

Meeting Started (9:00)

Announcements

(none)

Scout, Scout Packages, and Fall 2002 Solution Center CD-ROM (Kunz)

The MicroNet Scout for Windows underwent some revisions this summer for the first time in a couple years. Two major areas of the Scout Windows application were reworked – portable Scout-kit format (also used by the Solution Center CD-ROM) and the internal "Package installation directory" cleanup. Bugs were found in early Scout revisions (versions 5.3-5.5) due to the increasing number of operating system and file system types we need to test against. Version 5.6 seems to be very stable and is the version being burned on the Solution Center CD-ROM for Fall 2002.

Automachron (a network time synch application) is the only major new offering. Several people (due to some "clock drift" problems on some new systems) had requested a time-synch application. Automachron will not install "automatically" by Scout on Windows 9x class systems (but will auto-install on Windows NT and above). This is due to installer software limitations. The Win9x user will have the option to do a "manual" install (and click buttons and supply responses themselves) for Win9x installs.

Kunz remarked that "extraordinary efforts" will not be made now or in the future for older operating systems (such as Windows 95) to get products to work that will not (or cannot) work. However, Scout support for Windows 95 will continue for software that works with no (or a few easily solved) problems.

A copy of the new "Solutions!" CD-ROM (with new label artwork) was shown. It should be available by the time students begin returning in August.

ePolicy Orchestrator (Engholm, Balvanz, Day)

Dennis Engholm, Jeff Balvanz, and Al Day discussed current work by AIT on two new servers to support "ePolicy Orchestrator" ("ePO"). NAI's "ePO" is used to push out anti-virus policy and dat updates to departmental systems. A server is needed for the department with small client applications placed on the departmental systems (which contact the ePO server for updates and policy enforcement). The clients should not be able to circumvent the protection you enforce with ePO. Software for both server and clients is covered by the current NAI site license.

Two options exist for departments. First, you can buy your own server hardware and run your own ePO server. Second, you can contact AIT and share the extra capacity present on the two servers being developed by AIT. In the latter case, your department can apply your own policy and not be forced to accept what AIT has adopted. This will be offered as an "enterprise service". AIT is soliciting departments for participation during a "pilot period". The servers are hoped to be up by August 1, with "production status" by the start of fall semester. Some sort of "departmental admin" training is in the works.

Contact Dennis Engholm (dennis@iastate.edu) if you are interested in participating in the pilot project in sharing AIT servers.

Contact Al Day (alday@iastate.edu) if you want a copy of the client/server software to bring up your own system.

Contact Jeff Balvanz (jbalvanz@iastate.edu) if you need a grant number to get the software from NAI's site directly.

Questions: Mike Long asked if there was anything available in the anti-virus area for Palm or WinCE devices. Balvanz indicated the answer is "No, those products are not covered under the current license". Engholm indicated that if your department has an interest you should send email to him (dennis@iastate.edu) and such needs will be considered in the future.

SPAM Detection - PerlMX (Kunz)

AIT has purchased hardware and software to do "SPAM detection" on all inbound email. The product selected was PerlMX (this product was talked about in the last CCSG meeting). PerlMX will scan the headers of all inbound email (to "iastate.edu") and prepend a string similar to the following on the Subject line if the item appears to be SPAM:

> [SPAM DETECTED: #####]

The number of pound-signs indicates the likelihood the email is SPAM (the more pound-signs, the higher the probability). There is no "opt-out" for the Subject line modification. Filtering facilities on existing email packages can be used to detect the string and file/delete the email accordingly (it is up to the user to control what is done with the mail by their email application).

It is anticipated this new service will be available as early in fall semester as possible (depending on hardware availability, software setup, etc).

Questions: It was commented that PerlMX has the ability to actually delete the email. Kunz remarked that may be true, but AIT does not intend to get into deleting email, just marking possible SPAM for the user.

Upcoming Documentation (Kunz)

AIT has a couple new documents in the final stages of editing.

One document is an “ISU Net-ID Guide” that explains the system that exists for creating, suspending, and eventually deleting Net-IDs for students and staff. The timeframes and rules for such management are outlined, including interactions with Active Directory.

A second document is the “OU Administrators Guide”, which is a document based on the group of “quick and dirty tech docs” present at www.ait.iastate.edu/win2000/admin (but in a more organized - edited - format). Both of these documents should be available soon on AIT web pages.

Wayne Hauber (author of the “OU Administrators Guide”) solicited input from the OU admins on one section of the document still under development. A few examples of the use of Group Policy in campus departments that would be applicable to others on campus are needed. Current ideas are 1) a public lab for general ISU community login, 2) staff systems with restricted departmental staff login, and 3) a departmental printer with restricted access printing. Examples in use (or different examples) are solicited. If you have a good application of Windows 2000 and Group Policy in your department and would like to share it, please contact Wayne Hauber (wjhauber@iastate.edu).

Question: Greg Buttery (Business) asked if there was any response to the need for OU admins to be able to change the passwords for students. Bill Frazier (AIT) explained that the delegation of authority to do password changes for faculty/staff specifically tied to a department is allowed by enterprise design (and took considerable effort by AIT to support it). The same policy cannot be applied to students. Students typically use computer resources in several departments across campus during their course of studies. Allowing all OU admins to administer password changes for all students would result in a security compromise we cannot accept. This becomes particularly sensitive since many confidential services (such as AccessPlus access to grade and other personal information) may eventually be tied to the ISU Net-ID. There is no control of which people departmental OU admins may delegate such authority to. Greg indicated he did not necessarily need the ability to perform the operation himself, but was concerned that he had to send

Business students over to AIT to have a password reset. He wondered if something could be done via the phone (with support on weekends, too).

Rich Jones (ADP) agreed that this was as support issue that needed to be dealt with on the university level. This issue will be carried into other support services meetings within AIT.

Microsoft Campus Agreement (Hutchison)

Linda Hutchison discussed three issues relating the MCA.

First, there is a change in the CAL licensing portion of the agreement. Linda sent out an email to the CCSG (Kunz forwarded a copy to the WinAdmin mailing list after the meeting) that said in part:

> […]
> Some of you attended a session presented by Casey Niemann, ISU's Microsoft representative at the May CCSG meeting. At that meeting, Casey presented details of upcoming changes in Microsoft licensing. One of the topics he covered is the change in the CAL package included in the Microsoft Campus Agreement. Effective September 30, 2001 the BackOffice CAL package was no longer available with Microsoft Campus Agreements. ISU signed the current version 2.0 agreement in August 2001; version 2.0 included the BackOffice CAL. As such, ISU has the option to renew the agreement with the BackOffice CAL **for one additional year only**. The alternative is to renew the agreement with the package that is replacing BackOffice CALs - a package called Core CAL.
> […]

You should refer to this email (Subject: Microsoft Campus Agreement renewal - your input requested) for input into the decision solicited by Linda Hutchison at this time.

Second, AIT is working on software distribution mechanisms for the MCA software. AIT is setting up a domain “DFS” tree and will provide an access point for files (and possibly full-disk ISO images) of the MCA products via Windows 2000 authenticated connections. Kunz commented that one outstanding issue for the DFS structure is the establishment of an organization/naming convention for the DFS tree. This will be talked about at the next meeting (see “Windows 2000 – DFS” below).

Third, there have been changes to the “work at home rights” for staff under the MCA. Microsoft has extended “work at home rights” for all products covered under the MCA (including operating systems) to faculty/staff home systems. The products must still be used exclusively for “university work”.

Reminder: The web site for the MCA is at www.mca.iastate.edu for more details.

Questions: It was commented that systems using Matlab and SPSS (also covered under a site license) must be connected to the campus network.

Windows 2000 – Relocation OU (Kunz)

It was announced that a new "Relocation" OU exists for OU administrators to use to transfer objects (such as user-objects) from one OU to another. All existing OU admins have the ability to move users in and out of this OU container. This should be used when a staff member moves from one department to another, with one OU admin dropping the user object in the "Relocation" OU, and the new OU admin picking it up and depositing it in their OU. In this way the OU admins can handle the task quickly themselves.

Kunz reminded all that is it VERY IMPORTANT that OU admins not simply delete user-objects based on ISU Net-IDs, since a recreated user-object is NOT the same (they have different GUIDs). Many things (like decrypting encrypted files) will not work if a user object is deleted and re-created. They are "different users" even if they have the same username/password combination.

Windows 2000 – DFS (Kunz)

Work is being done to support DFS file sharing at the domain level for departmental admins. One of the features of the Active Directory design was that all OU admins should have the ability to add components to the DFS domain tree. One outstanding issue for the DFS domain shares is a naming convention for the tree to be used by the departmental administrators wanting to add shares to the enterprise. AIT will suggest a convention that will probably be based on college/dept names (similar to the OU tree model). This is desirable to prevent a very "noisy" flat name-space (which will be difficult to reorganize later after documents are created, links in place, etc).

This tree structure/naming convention will be a topic at the next WinAdmin meeting (July 26). If you have any other ideas on how DFS should be implemented, please send email to Kunz (skunz@iastate.edu) prior to July 26.

Windows 2000 – pswdutil Command Issues (Kunz)

Work on the new pswdutil command is nearly complete. This command will be used by OU admins to enforce some kind of password change policy on faculty/staff within their OU (either a list of specific usernames can be provided or the name of an OU container).

An interesting “design feature” by Microsoft was discovered in the process that is of concern at this point. When setting the “Account flags” for a user object you cannot set BOTH “User must change password at next login” and “Password never expires”. If you do try to set both flags, you will get the message “You have selected ‘Password never expires’. The user will not be required to change the password at next logon”. Since all ISU Net-ID user objects are created with “Password never expires” set, the act of forcing a user to change the password at the next logon means it MUST be also set to expire.

The default password expiration period for our domain is currently 42 days (the Microsoft default). Those of you who created local Windows exception accounts and did not set “Password never expires” discovered this. The situation now is that if the new pswdutil command is used to force a password change for a user, the LONGEST period that will be perceived by the user is 42 days. It is suggested a better domain password expiration period would be 180 days. OU admins can use the new pswdutil command to enforce shorter periods of time if they wish.

This change will be discussed at the next Windows Administrators meeting July 26. Any such change will only affect those accounts created without the “Password never expires” attribute set. Normal ISU Net-IDs will not be affected (UNLESS an OU admin sets the “User must change password at next login” flag either manually or with the new pswdutil command as noted above).

Meeting Adjourned (about 10:05)

Next Windows Administrator meeting is July 26. Be prepared to make decisions on the “DFS tree name convention” and “domain password expiration value” as noted above.