<div align="center">

Windows Administrators Meeting
May 9, 2003
Minutes (taken by Steve Kunz)

</div>

Meeting Started (9:05)

Announcements

- A reminder that the Windows Server 2003 2-day seminar will be held (for registered participants) next week on Monday and Tuesday.

- There are several "network events" coming next week (Monday morning). As previously announced via email, the IP number ranges for the residence halls are changing. Anyone who allows/restricts access based on raw IP number should be aware of the new ranges for the ".student.iastate.edu" subnets. In addition, "super-netting" will be implemented for the first time. In the past the netmask was always "255.255.255.0" for network segments. Every dorm may now have a different netmask. Friley Hall, for example, will be IP addresses 65.110.248.0 – 65.110.255.255 with a netmask of 255.255.248.0. NetReg (and DHCP) will automatically supply the correct values. In addition, the yearly "NetReg DHCP lease expiration" will happen for residence hall DHCP leases. The WINS servers will have stale residence hall and off-campus entries purged (on-campus entries will not be touched).

  Dave Orman (CNDE) asked out whether we should continue routing "10.10.*.*" addresses on campus. Steve Schallehn (Telecomm) indicated this is a policy issue since some departments may already have "on-campus-services" (such as web-servers) and rely on this routing to work.

- The "PswdUtil" and "ServicePackCheck" utilities were released in the "OU Admin Tools" section of the Windows 2000 Enterprise Support web-page (www.ait.iastate.edu/win2000/admin).

- The "Master Directory Sources" document is still stuck in "final review". It will be on the Windows 2000 Enterprise Support web-page when completed.

Spyware Removers (Kunz)

  Kunz discussed spyware removers and the pros/cons of offering them as ScoutKits. Spyware removers are a relatively new class of software used to remove executables, cookies, and scripts that collect and later report back information from the host system to someone. Many times a system has so much spyware on it that the system performance is degraded. Pop-up ads can appear when unsolicited/unexpected. The Solution Center had been using "Ad-Aware" in the past to remove spyware from systems. Because of licensing issues, "Spybot Search and Destroy" is now more popular. Another good product is "PestPatrol".

<div align="center">

1

</div>

Kunz talked about the difficulties of offering such a product as a ScoutKit. Spybot, for example, is bundled with an installer that Scout cannot automate. Configuration is problematic in that the wide variety of options (auto-updating, scanning, inoculation, etc) is not easily configured in a "one size fits all" scenario. Spybot is also basically written, distributed, and updated by a single person who may or may not keep up with the current pace of required updates. "PestPatrol" may be a better fit and stable product (especially for departmental use), but will require licensing research. "Ad-Aware" is another "more mature" product but requires regular "re-scans" (since there is no "inoculation" feature in the current version).

User Services support and "public relations" may be a problem with any selection of Spyware removers, since some products "break" when spyware components are removed ("Kazaa" is one example).

How Do You Set Up Printers for Labs? (Dave Orman, CNDE)

Dave Orman (CNDE) asked about setting up printers for labs. Some specific questions were:

- If network printers are dragged into the printers folder drivers are automatically installed and updated from the server at need, but they only show up for the user that did the dragging.
- If a printer is installed locally and then "aimed" at a network spooler it shows up for all users of that machine, but the driver has to be installed, and updated, locally.
- Is there a way to have computers in an AD group all show a given set of printers and set the default printer for that group?

Group Policy does not seem to provide an answer to these problems. Someone recommended a "kixstart" script to add printers to the system via a logon script applied to the system. Wayne Dowling (ECCS) indicated the Engineering College was using a "logon.cmd" script (which works well) but could not provide additional details.

Open Discussion

Greg Wilson (ISU Foundation) asked about garbled attachments when mail is sent from Outlook (Exchange) to a Eudora user. The version of Eudora (or the OS it was running on) was not known. Another person in the meeting had also seen this same behavior.
[**Information since meeting**: Outlook will use a Microsoft proprietary attachment of type "MS-TNEF". Mail clients from vendors other than Microsoft will not honor this non-standard attachment other than by following standard MIME processing rules. If you are sending mail from Outlook to a client such as Eudora Pro you should NOT

use the "MS-TNEF" format. Refer to the following Eudora and Microsoft KB articles for more information:
http://www.eudora.com/techsupport/kb/1552hq.html
http://support.microsoft.com/support/kb/articles/Q241/5/38.ASP
After some research, Greg Wilson discovered a setting to prevent an Exchange 2000 server from sending MS-TNEF attachments. In the "Exchange Server Manager" console, select "Global Settings", "Internet Message Formats", and "Default". On the "Properties" for "Default" select the "Advanced" tab and set "Never use" for the "Exchange rich-text format". Thanks, Greg! - SLK]

Russ Hoffman (Stat) asked if anyone was seeing problems with Veritas BackupExec 9.0 (on a Dell PowerEdge 4600). BackupExec seems to lock up when backing up the full system partition and system state. One other person in the meeting reported the same problem. Previous versions (version 8.6) did not exhibit this behavior.
[**Information since the meeting**: Russ provided additional information in a follow-up post the CCSG mailing list. See below – SLK]

Jim Wellman (AE EM) warned that OpenAFS would remove a file (or folder) if you deleted a link (instead of just removing the link). Kunz remarked that this has been "standard behavior" for Transarc AFS from the beginning.

Jim Wellman (AE EM) also asked if Durham 171 had wireless available for the Windows Server 2003 session next week. The answer is "Yes".

Jim Wellman (AE EM) asked if there was any decision on offering a local Windows Update Server (for hotfixes, service packs). Kunz commented that this issue has been raised several times in the past, seems like a good idea, but is currently inactive due to lack of staff time.

Dave Orman offered some info on "secure departmental FTP servers" (where the password does not go over the wire in "clear text"). Dave tried SSH.COM's product and did not like it. He currently likes "SurgeFTP", which is an "SSL FTP" product. It can encrypt both the authentication and data streams and costs about $300 per server. The main limitation is that is can only perform the SSL encryption when connected to by FTP clients that have SSL incorporated. Some products mentioned are "SSLFTP", "FileZilla", "HeadShot", and "WSFTP Pro" (the "for purchase" version of "WSFTP LE" distributed by Scout).

Steve Kunz (AIT) offered a couple tips for those people looking to recover some space on their Windows 2000 system partition (normally "C:"). Back when Windows 2000 came out many vendors were shipping pre-config'd systems with a 2 GB "C:" system partition. Hotfixes and services packs have been slowly eating that up. Repartitioning (whether via products such as PartitionMagic or backoff-restore rebuilds) is one method. A second alternative (for the "cautiously brave") is to follow the advice in Microsoft's Knowledge Base Article "290402" (at http://support.microsoft.com/?kbid=290402). It is possible that by moving the

"service pack files" folder (where the last service pack is stored) and the "service pack backoff" folder (for removing service packs) to an alternate volume you can recover up to 500 MB of space on the default "C:" system partition. This process involves moving system folders and altering registry entries. As usual, GREAT CARE SHOULD BE TAKEN. If at all possible, experiment on a disposable system first! Have a backup!

The folders (if they exist) reside at the following locations:

- C:\WINNT\$NtServicePackUninstall$ (hidden system folder)
- C:\WINNT\ServicePackFiles

You can examine these folders and see if they offer enough space to warrant the effort. Kunz chose to NOT delete the "$NtServicePackUninstall$" folder (as indicated in the KB article) but moved it to a second partition and updated the registry entry with the new location. It is further recommended that you first only move the "$NtServicePackUninstall$" folder (and leave "ServicePackFiles" where it is). This is the safest move and may easily buy you enough space for a while.

If you chose to try this, follow the steps in the Microsoft KB article mentioned above. Kunz recommends a "best practice" is to create a "WINNT" folder on another partition (for example, "E:\WINNT") and move the folder(s). Place within this new "WINNT" folder a TXT file named "DO NOT REMOVE THIS FOLDER.txt" with an explanation of the files and registry entries relating to them (so you later do not think it is a "leftover" from something else). Next, edit the registry as per the KB article (you only need to change the drive letter if you created the "WINNT" folder) for the folder(s) you moved. Finally, SCAN the entire registry for strings with the old value so you can change all places (the KB article misses some).

Again, NO WARRANTY supplied for this advice. Kunz has used it on a few systems with no problems. Experiment at your own risk.

Meeting Adjourned (about 9:50)

Next meeting is June 13.

Additional Information
Veritas' Backup Exec 9.0 on a Windows 2000 Server

```
[The following information is from a post Russ Hoffman made to the CCSG
mailing list regarding his problems with Veritas Backup Exec 9.0. Russ
has kindly granted permission for me to reproduce a portion of his post
here. - SLK]

Problem number 1: The backup would fail after backing up 10-12Gb. The
system generated the following error messages, "Warning - A severe
```

error occurred while reading or writing data. This job may not have been successfully completed. Critical - The tape is from a faulty batch or the tape drive is faulty:"

Solution:
In this case I had two consecutive bad tapes right out of the box - which caused some confusion as to whether the problem was with the device or the media. However, to confirm that it was indeed the media, in BE under Media, tape properties, Statistics, there is a section that shows the number of seek errors, soft & hard read errors, and soft & hard write errors. If there are any seek, or hard read or hard write errors, then the media is considered defective - according to Maxell support. BTW: I've now tested 14 tapes and have found 3 bad ones - not a great track record for Maxell in my opinion, but they said they would exchange them no questions asked.

Problem number 2: The backup seems to complete a backup but hangs at 99% and the only obvious way to clear this job is to reboot. More specifically, it only does this when the "Eject media after job completes" option is enabled.

Solution:
First, there's no need to reboot - all that one has to do is to find and acknowledge the alert message that tells you to remove the media from the drive (that's already been ejected) and respond OK. However, the real problem is a configuration issue.

This is a case where a handful of settings have to be checked and/or set. Start with a program called ...\VERITAS\Backup Exec\NT\BEUtility.exe, specify the server, choose "Edit Configuration" under the Services Tasks, set the "Automated Alert Responses" to "Yes or OK" - especially the media remove alert.

In BE, under the Alerts tab, Alerts Tasks, Configure alert categories, find and highlight the Media Remove category, then enable the "Automatically clear alert after..." option and set the time value to something very short - for example, 1 minute.

Last, in the backup job properties, enable the "Eject media after job completes" option. With that, and a bit of luck, you should be able to successfully run backup jobs and automatically eject tapes upon completion.