**Windows Administrators Meeting**
May 24, 2002
Minutes (taken by Steve Kunz)

## Meeting Started (9:05)

## Announcements

- May 21 – Windc3, a third root domain controller, went into production service. This system is housed in ADP's machine room (for multiple physical site dispersion of critical controllers). We now have two "global catalogs", giving us the ability to take any root domain controller down for maintenance with no "down time" perceived for authentication services. Admins are cautioned not to manually configure clients to authenticate to a given domain controller, because if that one is taken down they may not automatically fail over to another one available in the enterprise.
- Security monitoring is being automated for failed attempts at key enterprise accounts (such as the enterprise administrator accounts). Malicious (large volume) hacking attempts at powerful domain accounts will be turned over to AIT's Security Officer. There are many instances of "low volume" attempts, which appear to be some artifact of how Windows attempts authentication to join a machines to the domain. Analysis of what is exactly happening here is still under way.

## IBM/Transarc AFS Client Bugs

The IBM/Transarc AFS client for Windows NT/2000/XP being distributed via an "advanced" Scout-kit is version 3.6 patchlevel 2.18. This version has a bug in it that causes the client to absorb almost 100% of the CPU if the local network connection goes down. This bug is fixed in the current version of the client, version 3.6 patchlevel 2.32. However, this version has another bug that prevents the saving of roaming profiles in AFS under the "ISUGina" system. An effort will be made to report the latter bug to IBM/Transarc before the latest version of the software is released.

## Comcat.dll Problems

Microsoft released a "security rollout" hotfix in April that updated the "comcat.dll" system file and broke a critical "DLL registration" process. Moving some functions from "comcat.dll" to another DLL and "forwarding" the calls to the second DLL created this condition. They distributed updates to "comcat.dll" and not the second DLL (so the "forwarding" fails).

One obvious way to know if your system is in the "broken comcat.dll forwarding" state is to use Internet Explorer 4.0 or later and try to display a ".pdf" on a web site (other web-site pages may also exhibit this behavior). If your IE browser displays the error message "This page provides potentially unsafe information to an ActiveX Control. Your current security settings prohibit running controls in this manner. As a result, this page may not display correctly" you are probably in "DLL Hell".

Microsoft has a Knowledge Base article on this topic (and how to fix the problem) at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q201364

### Domain Policy Change – Set Date to Change "LMCompatibility Level"

The issue of LANMAN and NTLM protocols being used for authentication was continued (see the meeting notes for the March 8 and April 26 meetings).

At the April 26 meeting, the final decision was made that it was probably safest at this time to go to "Level 1" protocol negotiation on the domain controllers (negotiate to use NTLMv2 and fall back to the other lower protocols if the client cannot do it). This is recommended in SANS documents if the higher security setting causes problems (like it will here). We had not previously set a date for this change.

At this meeting it was decided to make the domain policy change on Wednesday, May 29, 2002. An email announcement will be made the day before (to the WinAdmin mailing list). Email any problems that seem to relate to this change to skunz@iastate.edu starting May 29. There SHOULD BE NONE, since all existing protocols should still work. This will just enable higher security to be negotiated.

### Domain Policy Change – Re-enable the "Change Password" Button

One of the few domain policy changes implemented two years ago was the disabling of the "Change Password" button on the "Ctrl-Alt-Del" security screen on client systems. The reason was because password changes in Windows were not "synched" back up to Acropolis, so all password changes had to come from Acropolis (and by synched down to Windows).

On April 23, the "bi-directional password synch" was installed and this restriction is no longer necessary. Since no problems have been seen in the software since that time, the "Change Password" button can be re-activated for the users. If you do not want your client systems to have this ability within your OU, you can always reapply your own group policy to disable the button (although this is not recommended unless absolutely necessary).

At this meeting May 28 was established as the date to re-enable the "Change Password" button.

### WinAdmin Meeting Schedule for Coming Year

Kunz announced he would be unavailable to chair any WinAdmin meetings during June. Since nobody else saw the need to chair a meeting, all June 2002 WinAdmin meetings are cancelled.

Discussion turned to scheduling WinAdmin meetings for the coming year. Kunz asked the question as to whether or not two meetings a month were necessary for the Windows Administrators group. It was decided to move to “one meeting a month” on the “second Friday, 9:00-10:00 AM”. The room will also be reserved for the “fourth Friday” but a meeting will only be scheduled at that time if the “second Friday” meeting deems it necessary. Any such “extra” meetings will be announced via email (with the topic).

## Open Discussion

Problems with Scout-kit Xnews installs on Windows XP systems were brought up. It appears that if the user is an Administrator (or power user) they can install and use Xnews with no problems. “Normal” users, however, do not have the rights to install certain control files in the default locations. Kunz said this issue will be brought up with the MicroNet Group for resolution.

## Meeting Adjourned (about 9:30)

Next Windows Administrator meeting is July 12 (“second Friday” in July, no meetings in June).