Windows Administrators Meeting

May 12, 2006

Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- Annual networking changes occurred May 8. This included regular yearly cleanup of NetReg and WINS databases for residence hall systems. A short DNS outage on one DNS server and a backlog of NetReg processing that day were the only problems that occurred. Both problems will be fixed for next year's event.
- LANMAN and NTLMv1 were disabled 1:00 PM May 10, 2006 as announced.

Effects of Disabling LANMAN and NTLMv1 – Kunz (ITS)

Kunz gave an overview of problems reported to ITS after LANMAN and NTLv1 were disabled via domain policy on Wednesday, May 10. Most reported problems centered on Samba servers (either Linux or Mac OSX 10.4). Jim Wellman (AER E) reported that they did have a problem with a Ricoh "copier/scanner" that they circumvented by switching to a non-domain (local to the server) account.

As previously announced, Samba 3.0.14a is the earliest version that apparently has no problems (Samba 3.0.22-1 is the current version for RedHat Linux). Some people have reported that even Samba 3.0.10 server can function with the proper configuration. The following settings are recommended:

Relevant smb.conf settings on a Samba 3.0.10 server:

security = ADS
realm = IASTATE.EDU
use spnego = yes
encrypt passwords = true
passdb backend = tdbsam guest
password server = windc1.iastate.edu

[Kunz noted it would be best if everyone did not chose "windc1.iastate.edu" as the "password server" for load balancing and "single point of failure" issues]

Since no major problems have been reported with the new policy settings the decision has been to retain the current policy. It is recognized that some people may have been gone this week and new problems may be reported next week. Should any change be required it will be widely announced. People with continued Samba problems are encouraged to use the WinAdmin and Mac OSX lists to work on configuration or upgrade issues.

Enterprise WSUS Server Proposal – Kunz (ITS)

Kunz encouraged discussion of the "WSUS Server Proposal" in which "client side targeting" might be used to filter out some updates to systems via group policy settings (see http://tech.ait.iastate.edu/win2000/admin/WSUS_Prop.05.09.06.pdf).

In general the people in attendance were in favor of the new “SC” (“Security and Critical” updates) group. However, during the discussion several people were in favor of not providing driver updates to the “Unassigned Computers” group (the default group if no group is specified by the client-side group policy settings). The reasoning for this is that driver updates are probably the single most problematic update and are probably best applied by a system administrator on an “as needed” basis. Video and network drivers have stung several IT admins in the past.

In the end the “WSUS Server Proposal” was recommended to be altered to 1) remove drivers from the Unassigned Computers (default) group 2) retain the “SC” group as is and 3) create a third group named “All” containing all possible updates (including drivers). This means current systems pointing to the WSUS server would have to use client-side targeting to get driver updates (if they want them via the WSUS server).

The proposal document will be altered and a new email containing the changes will go out to the WinAdmin list early next week. Hopefully we can get this support up very soon after brief discussion.

Open Discussion

Steven Spencer (PSYCH) commented that there is a security flaw warning about VNC. He will post information about the warning to the WinAdmin list.

Russ Hoffman (STAT) asked about GPO settings for servers relating to WSUS updates and reboots.

Jim Wellman (AER E) asked if anyone else was seeing problems with “supernetting” changes this week. He was referred to the DNS people for further assistance.

Jim Wellman (AER E) gave a warning about problems created when “User GPO” is applied to a staff person in one department who then logs into systems in another department. The GPO settings may have adverse effects in the alternate location. Kunz commented that this is generally why “loopback processing” is applied (so that machine GPO settings can be used to set user policy settings for all users that login to a system).

Meeting Adjourned (9:55)

Next meeting is scheduled June 9, 2006