Windows Administrators Meeting

March 8, 2002
Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- The WinAdmin email list has had some bounces because of forwarded mail to "@home.com" addresses. If your mail is forwarded to an "@home.com" address you have been dropped from the list. [Aside: Of course somebody else will have to tell you this, because you are not receiving email.]
- The CIRAS child domain was shut down after a successful conversion to a "CIRAS" OU. [Thanks to Chris Thach for his cooperation!]
- The E500 central anti-virus email filter has been in service for about a week and a half. As of last weekend it had filtered/cleaned 800-900 infected pieces of mail. There was some discussion of how infected mail could still enter the campus. There are still "holes" in the enterprise mail structure that need to be plugged (as widely announced) on March 26. In addition, mail that bypasses the central mail servers and goes directly to departmental mail servers will still be susceptible to infection.

TechNet Presentation (Kunz)

Steve Kunz and Greg Wilson talked about the Microsoft TechNet held in Des Moines on March 6. The main topics presented were:

Microsoft Operations Management ("MOM")

This is a client/server system offered by Microsoft to monitor your systems and detect problems, providing alerts and reports to systems administrators. This product was developed by "NetIQ" (based on NetIQ version 3.3) and adopted by Microsoft. It can monitor up to 600 systems, has 710 "rules" enabled by default (with 11,000 possible). System events and event-logs can be monitored automatically. Retail cost is $850 per system monitored. Kunz remarked that AIT is already using a shareware product called "Big Brother" to monitor AIT systems in the machine room (Unix and Windows). Big Brother monitoring of Windows 2000 systems is currently very limited. Microsoft says MOM will monitor NT 4 systems but it is "not as robust". Clients are installed on each system that needs to be monitored, and central monitoring/administration for the whole enterprise is the core design. Microsoft has a "white paper" on using MOM in "complex computing environments" where departments may want to monitor their own systems individually (enterprise control is not a requirement to run MOM).

Federated Server

This is a Microsoft offering where a local server can be used as a distribution point for Microsoft security patches and hotfixes. The "Windows Update' feature on the Start menu and IE Browser will then communicate with the local store for updates. The manager of the local server can make any hotfixes available locally only after "testing and approval" if they so wish. Since AIT has already successfully used locally caches copies of other products (like the NAI virus definition DAT files) this may be something we could offer (especially when important hotfixes make load and network problems for the Microsoft-based servers). The "testing and approval" process would have to be coordinated if implemented here, and hardware/setup would have to be investigated. No commitment is made at this time by AIT (it has some manpower implications).

LANMAN and NTLM Authentication Concerns (Kunz)

Kunz talked about the problem with older authentication/encryption protocols being used in the Windows 2000 root domain. "Backlevel" protocols are supported by default on all Windows 2000 domain controllers, meaning they will authenticate with LANMAN, NTLM, and NTLMv2 protocols (in addition to Kerberos V5). LANMAN is mainly used by Win9x systems. NTLM was used by Windows NT 4 prior to SP4. NTLMv2 was available on NT 4 after SP4. LANMAN and NTLM are extremely vulnerable to cracking and are not recommended to be used in our environment. The domain controllers can be configured (by a domain-wide group policy) to only communicate with NTLMv2 or Kerberos V5. NTLMv2, while not as secure as Kerberos, can use 132 bit encryption techniques and can be considered "minimally acceptable". However, if this rule is enforced then authentication used by any current "backlevel" clients will break. The question is, "How many of the ISU Windows community would this affect?" This will affect you if you have made older NT 4 systems members of your OU or if you have made Win9x systems a member of the IASTATE workgroup. [This is NOT recommended at this time due to this issue]

Should the rule "NTLMv2 and above" be enforced, there ARE things you can do to older systems to allow them to authenticate to the root domain. NT 4 systems can be patched to current patchlevel (SP6a) and be able to authenticate with NTLMv2. Windows 9x systems can install the "Directory Services Client" on them (but is was reported this may not work on Windows ME). The installer is available off the Windows 2000 CD-ROM at "Clients\Win9x\Dsclient.exe". A Dsclient.exe installer is also available from Microsoft for Windows NT systems. In addition to installing NTLMv2, it also allows the "Find" command to function with Active Directory (allowing you to find people, systems, printers, etc).

Discussion of this issue will continue in a future meeting. More detailed information on this issue is available in the following Microsoft Knowledge Base articles:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q239869
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q147706

Open Discussion

Jim Wellman (AEEM): In relation to the "MOM" discussion, some people used to use XPVwatch to monitor departmental systems (but that was shut down with the SNMP security hole concerns). He asked if any central monitoring tools can be agreed upon and made available. Bill Frazier (AIT) responded that this had been looked at periodically in the past, and many times the large cost is the biggest issue. However, he will look into what can be done (with whatever tools we have available or can get) again. [No timeframe promised]

Mike Long: Asked if the current budget cuts will affect Win2000 support? Frazier (AIT) and Kunz (AIT) said as far as they know the answer was "No, Windows 2000 is considered a core service offering". Kunz stated a third (and possibly fourth) domain controller are being planned to handle projected increased load (and meet the AD Design Project recommendations).

Reminder

Barbara Borrowman from Network Associates will be on campus demonstrating their anti-virus software management tool "ePolicy Orchestrator". She and her sales engineer will also be available to answer any questions regarding this tool and other McAfee products after the presentation.

The presentation will be:

```
Friday, March 15th
9:00-10:00 AM
Durham 144.
```

Meeting Adjourned (about 10:00)

No Windows Administrators meeting on the “fourth Friday” of this month (Spring Break).
Next Windows Administrator meeting is April 12.