Windows Administrators Meeting
May 13, 2005
Notes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- Changes announced for week of May 9 happened. See: http://tech.ait.iastate.edu/win2000/admin/Announce.05.11.05.pdf

- AIT will be increasing the default AFS quota to 1 gig on June 1, 2005. Currently the default AFS quota is 500 meg.

- The Windows OpenAFS 1.3.8201 client has been released on the "Advanced" Scout-kit list. Users of the Windows AFS client are encouraged to upgrade to this latest release, as it has quite a bit of maintenance work applied to it.

- Steve Schallehn (TEL) said users will begin to see digital certificate "expiration" warning notices for the Cisco VPN client software. When certificates were issued last year they were valid for a year. As they approach expiration the VPN client will begin issuing warning messages. AIT will announce proper procedures for updating the VPN client certificates in the near future.

- Beata Pruski (AIT) said the JMP license renewal process has started. The license will expire June 30 (but there is a 30 day grace period with warning messages after that). As in the past, we will get the new license out at soon as possible. Watch for further announcements in the email support lists.

- Steve Schallehn (TEL) said a backbone upgrade is in progress. We are back in stable mode after recent maintenance. "Network Maintenance" announcement have been going out the email support lists.

Class List Status

Kunz gave a status report on the "Class-List" project (pushing class-lists down as Windows Global Security Groups). This project is close to "going production". Next week (the week of May 15) AIT will begin pushing down the departmental, major, college, and "Summer 2005" class lists (those created by ASW instructor action).

Kunz cautioned everyone to not immediately begin using these new security groups as soon as they appear. Should problems appear in the process AIT reserves the right to make the groups "disappear" without notice. Wait for a formal announcement.

Kunz thanked Chris Gray (AGRON) and Stephanie Bridges (ECON) for participating in preliminary testing. During Stephanie's testing it was discovered that the Microsoft "ifmember.exe" utility is very valuable in logon scripts to determine group membership in a FERPA-compliant way (to control drive mapping, etc). This product was already documented with the aid of Sudhakar Chinnaswamy (Office of Sponsored Programs Administration). See: http://tech.ait.iastate.edu/win2000/admin/groupawarescripts.pdf

Digital Certificates (PKI Infrastructure)

Kunz brought up the "Digital Certificates" topic from the email support lists and the last CCSG meeting. The request for a digital certificate server in the Windows Enterprise domain has been introduced within AIT as a possible new Windows Enterprise domain service. Kunz indicated that this possible service would be part of a larger "PKI Infrastructure". One possible model would be the Windows cert server being a "subordinate" to an Enterprise open-source "Root CA" (possibly OpenCA). The easiest for users would be to buy root CA services from a commercial vendor (Thawte, VeriSign, etc) but this is very expensive. Considerable study will have to be done first to decide the best way to go. We definitely want to design this infrastructure right from the start, so it is nicely integrated in a heterogeneous OS environment.

Kunz solicited needs for digital certificates in the Windows environment. A beginning list consists of:

- Wireless LAN (802.1x)
- Smart Card Logon
- Secure Files (EFS – data encryption)
- Secure Messaging (Encrypted/signed email)
- Document Signing
- Web single sign-on
- LDAPS (Secure LDAP)
- IPSec (machine communication)
- HTTPS/SSL
- Access

Kunz highlighted the "auto-enroll" features of Windows Active Directory, where AD Group Policy can be used to enroll users and automatically renew certificates for services. This takes much of the drudgery (and user learning curve) from certificate management. Active Directory will store some digital certificates with the user objects.

AIT has begun internal discussions on a PKI infrastructure. We will keep you posted as the research continues. Watch for further discussion in both the WinAdmin and CCSG meetings.

Open Discussion

Kunz said someone had asked him about the possibility of getting Windows event log help from people who had solved problems as flagged in the event logs. Perhaps a database (or at least a list) of events and what you do in response to correct the problem. The general consensus was the WinAdmin mailing list could be used to ask the question and get any answers from the group. Kunz volunteered to collect the final answers and place them in the tech support web pages as he saw them in the list. This can be ongoing. People should also note there are several good web-sites out there that can provide help (places like http://eventid.net).

Jim Wellman (AER E) asked if anyone else was seeing a problem with time synchronization. Some client systems apparently cannot synchronize the time with the domain controllers. One or two other people had seen similar problems in the past. This will probably take some event log analysis and research. Wellman will pass on some event entries to AIT.

Meeting Adjourned (about 10:10)

Next meeting is scheduled June 10