Windows Administrators Meeting
December 12, 2003
Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- Kunz reminded everyone of the upcoming "security tightening" that will occur January 6, 2004. At this time the Kerberos 4 authentication port will be disabled (forcing "Kerberos 5 only" authentication). The recent upgrade of several Scout-kits relate to this security upgrade. See:

  http://www.ait.iastate.edu/security/encryption/

  for detailed information on the Jan 6, 2004 Kerberos 4 shutdown and security tightening implications.

- AIT is considering discontinuing Usenet News service. An email announcement was sent to the IT admin support mail lists on Dec 11 with the subject "Request for Comments: Discontinuing Usenet News Service". The same information is available at http://www.ait.iastate.edu/showitem.php?id=95. Comments should be sent to usenet-comments@iastate.edu by January 7, 2004.

- Kathy Jones (Office of the Registrar) gave a good presentation on FERPA compliance at the last CCSG meeting. Two good documents from the Office of the Registrar are:

  http://www.iastate.edu/~registrar/info/ferpanotice.html
  http://www.iastate.edu/~registrar/info/confid.html

  In addition, a handout titled "FERPA: What faculty and staff members need to know" was handed out at the CCSG meeting. Refer to the CCSG minutes (or contact the Office of the Registrar) if you need further information.

Windows Domain Controller Upgrade Plans (Kunz)

Kunz gave a status report on the upgrade plans for the Windows Enterprise domain controllers. The upgrade project was approved and hardware for WINDC1, WINDC2 and (the new) WINDC4 has arrived. The infrastructure upgrade is a joint project funded and staffed by AIT (WINDC1 and WINDC2) and ATS (WINDC3 and WINDC4). These replacement systems have:

Dual 300 Ghz processors
Dual power supplies
2 GB RAM

RAID5 three-stripe + 1 hot spare
SDLT tape backup
100 MB Ethernet
Windows 2003 Server OS

Kunz said that remarks made in the last WinAdmin meeting have influenced how we will perform the upgrade. The original plan was to introduce new hardware as WINDC1A and WINDC2A (with new IP numbers) and then decommission WINDC1 and WINDC2. This would affect people with personal firewalls on member systems, since you need to punch through holes to the domain controllers for domain authentication. After considering the pros/cons, AIT and ATS have decided a new plan. We will introduce WINDC4 first (giving a mixture of Windows 2000 and 2003 DCs) and check for stability. Next we will transfer DC roles from WINDC1 to WINDC2-4, remove WINDC1's domain controller roll, and shut it down. We will then configure a new system as WINDC1 (with the same IP address) and reestablish its role as a domain controller. The same procedure will be followed for WINDC2. Finally, WINDC3 will have an OS upgrade. At this point we will be in a "pure Windows 2003 Server" Domain Controller environment.

A "schema change" is needed to introduce Windows 2003 Server domain controllers. We will be doing this sometime during January/early-February 2004 (certainly *after* January 5, 2004). The reason for the delay is two-folder. First, we would like to offer stability for departmental IT admins during winter break to their between-semester work. Second, that we have been told by other university sites that the schema update can be problematic if OU administrators have changed security attributes on OUs that can prevent the schema updates from touching all objects in the domain. Microsoft itself has found this to be problem and recommends "dry runs" in an isolated lab environment that has been created from a backup of the production domain. AIT/ATS will be doing these "dry runs" in our Windows test lab. If we encounter any problems in the test lab we will be contacting the departmental OU admin to assist in allowing the schema updates to be successful in the production environment. This process will be repeated until we have a clean "dry run" in the lab. At that point we can schedule the production schema updates. We will be performing the Exchange 2003 schema updates at the same time.

One other issue that is raised by the introduction of Windows 2003 Server domain controllers is the fact that "SMB Signing" will be enabled by default. According to Microsoft Q-article 325327 (http://support.microsoft.com/?kbid=325379):

> "Local security settings defined on Windows Server 2003 domain controllers require clients to use SMB Service signing. Windows 95 without the Active Directory directory service client installed and Windows NT 4.0 Service Pack 2 (SP2) or earlier clients are not compatible with the SMB Service signing requirements that are enabled in the default Windows Server 2003 security settings. Such clients cannot authenticate with, or access resources on Windows Server 2003 domain controllers."

We do not intend to change this default action. Windows 95 systems that must use file/print sharing to domain-member systems can install the directory service client (available from a Windows 2000 Server CD in the I386 folder). Windows NT 4 systems should update to SP6A. We are unclear of the implications for Mac OS9 and OSX systems in our environment (though we suspect Mac OSX systems will be fine). We will experiment in our lab and provide more information as we know it.

Open Discussion

Kunz asked about experiences with the blocking of Windows file/print-share ports at the border and the new VPN service. Kunz commented that Intrusion Detection Systems indicated a sharp drop (nearly to zero) of automated hack-attacks against accounts in our domain. Steve Schallehn (Telecommunications) commented that VPN server usage has been "very low".

Kunz commented that there has been a request for information on a VPN client that works on Mac OS9 systems (Cisco only provides a client for Mac OSX). A third-party product apparently exists but has not been tested. Interest was expressed in a VPN package for PocketPC on the CCSG mailing list. [Information since the meeting: Dan Sloan (VetMed) indicated on the CCSG mailing list that "MovianVPN is recommended by Cisco. $41.98 through our university contract with Insight Direct. Its available for both Palm and Pocket PC based systems."]

Frank Poduska and Wayne Hauber (AIT) talked about a couple issues they have had reported through the Solution Center. Apparently on some "low-end" home router boxes you can only have one system doing VPN at a time. Another issue arises on home systems doing Microsoft's "Internet Connection Sharing" (ICS). You cannot activate the VPN client on the system managing ICS (but you can do VPN on any of the "downstream" systems from the main ICS system).

Kunz solicited ideas on topics that could be discussed in future WinAdmin meetings. Any IT admin functioning in our forest/domain that feels they have a procedure or technique from which others could benefit can provide documentation or be provided some time in future meetings. Just send email with your offering to skunz@iastate.edu. Ideas suggested in the meeting were:

- How to set up Outlook and Novell client software on home systems
- How to set up saving "favorites" in a lab environment (and other shared-lab or public system ideas)
- Using Dell "OpenManage"

Meeting Adjourned (about 9:55)

Next meeting is January 9.