Windows Administrators Meeting
September 13, 2002
Minutes (taken by Vince Oliver and Steve Kunz)

Meeting Started (9:05)

Announcements

- Al Day, a full-time staff member from the AIT Labs Management Team, has replaced Troy Frette as one of the three Windows 2000 Enterprise Administrators.

- Steve Kunz and Andy Weisskopf (both members of the AIT Systems Group) will attend an all-day SANS seminar on September 23 titled "Gold Standard Security Benchmark Training – Securing Windows 2000". This session will cover "best practices" for securing Windows 2000 systems developed by the Center for Internet Security, DISA, NSA, NIST, SANS, and GSA. Kunz will devote a future WinAdmin session (or sessions, if need be) to getting this information out to others at ISU.

Service Pack "Blues" (Kunz)

XP SP1: Kunz referred to the WinAdmin/CCSG mail-list discussions on the release of Windows XP Service Pack 1 and ramifications seen by some already. It has been reported this service pack alters the XP "Activation" rules, interferes with SAMBA server usage for the storage of roaming profiles, and may break ZoneAlarm Pro. HOWEVER, it was also noted by Steve Kovarik (E CPE) that this service pack patches some critical security holes and it is considered very important to apply.

2000 XP3: Kunz reported that all three root domain controllers (running Windows 2000 Server) had Windows 2000 Service Pack 3 installed on Sept 3. No serious problems were detected (although one instance of the NetShield driver crashing a DC occurred the following week that is as of yet unexplained and has been reported to NAI). Steve Heideman (CHEM) had some problems with "file protection errors" at login to some servers he applied SP3 to. A "freshly built server" (without a previous history of hotfixes prior to SP3) does not exhibit this problem. It was suggested (from the audience) a profile rebuild be tried on the "problem" servers.

IE6 SP1: Kunz told a personal story of installing this on his home Windows ME system, being unable to read HotMail, and have HotMail consulting inform him they have "confirmed the problem with Technical Support" and suggested he "uninstall IE6 SP1" for now. Upon doing so, the "uninstall" failed after reboot, leaving the system in a mode where it "hung" after login (desktop background appeared, then system lockup). SafeMode was also non-functional. Final result was to rebuild the system. Kunz (in hindsight) wishes he would have used the Windows ME "System Restore" (instead of IE6 "uninstall") to back level his

system to a state prior to IE6 SP1. No other people in attendance had experienced any such problems. [Note: XP SP1 includes IE6 SP1]

Kunz commented on the good use of the WinAdmin (and CCSG) mail lists in answering people's questions. Please keep sharing information.

Exchange 2000 Status (Kevin DeRoos, ADP)

- Exchange 2000 has been installed on ADP's new Exchange servers.
- CARD's Exchange 5.5 organization/site has joined ADP's Exchange 5.5 organization/site in preparation for Exchange 2000.
- An "Active Directory Connector recipient connection agreement" was created this week and then removed. The removal was necessary because it created duplicate user objects for all Exchange 5.5 users within Active Directory. The ADMT ("Active Directory Migration Tool") needs to be run first. The duplicates were cleaned up.
- Steps to be followed are to first "mail-enable" all NetID-based user objects in Active Directory, run ADMT on all Exchange 5.5 accounts (merging the info with the user objects in Active Directory), and finally re-establishing the "Active Directory Connector recipient connection agreement". A final step will be to move the SMTP connector from Exchange 5.5 to Exchange 2000.
- Vince Oliver noted it is VERY IMPORTANT for existing Exchange 5.5 sites to join in the migration process prior to us switching the Exchange server organization from "mixed" to "native" mode. After going to "native mode" any Exchange 5.5 server wanting to migrate will need to do so on a (painful) user-by-user basis.
- Contact Kevin DeRoos, ADP (kderoos@iastate.edu), when your department is interested in joining our enterprise Exchange 2000 organization.

OU Privileges/Security Issues for OU Admins (Kunz)

Kunz mentioned the web-base documentation changes (an companion email sent out to the WinAdmin mailing list) about "locking out" enterprise access to departmental OUs. This practice of securing OUs is NOT discouraged UNLESS it interferes with portions of the enterprise AD design. In the case of locking out changes to NetID-based user objects by enterprise administrators, attribute and password changes could not longer be done by automated processes run at the enterprise level.

Refer to the web-based documentation for the rules concerning access to containers with NetID-based user objects. Kunz encouraged anyone who is working with "locking down" security in OUs to document and provide feedback (to either this group or Kunz) on what they had successfully done. Other OU admins may be interested in these techniques and we will document those that achieve the desired affect without breaking the core elements of our AD design.

User Object Management Guidelines for People Leaving Your Department (Kunz)

The automation that happens to deposit faculty/staff user objects into an OU are well documented and in place. Over the past few months, however, the question of what happens when a faculty/staff member leaves the department (by either leaving the university or moving to another department) has come up. Kunz said he has erroneously told a few OU admins to simply "disable the user account and leave it in your OU". However, when the user object is based on a NetID, that is not the correct action. A person may leave the university and come back as a student (or they may simply transfer to another department). Since their NetID is still valid, we want their Windows 2000 user object to be the same object (same GUID) and still valid.

The "Relocation" OU is the proper way to "dispose" of NetID-based user objects contained in your OU (when you have decided they should no long be your responsibility or inherit your policies). You should move these user objects into the "Relocation" OU. At that point you should send email to its-ad-admins@iastate.edu and indicate what user object you just placed into "Relocation" and a brief reason as to "why" ("left the department", "left the university", etc). The enterprise admins will move the user into an appropriate container. If you know an OU administrator (and an OU exists) for the department a person is transferring to, you could move them into the "Relocation" container and notify the person's new OU admin that they can pick them up. However, for the near future most transfers will probably be back into containers reserved for the "General User Pool" (which only the enterprise admins can do).

Special care needs to be taken if a staff member leaves and they are still members of security groups you have created. Even if the user object is placed in the "Relocation" container, the access applied by "group membership" is retained. You must remember to remove them from any "groups" you have created. Similarly, if you have specifically altered the ACLs of containers, objects, etc. for access by a specific user you should clean these up (this assumes good change-documentation on the OU administrators part). Remember – if any privs are granted simply by OU membership (Group Policy applied to an OU container where the user object resides) then they lose those privs automatically when they are moved outside the OU.

Keeping Many Systems Up to Current Hotfix Level

A question was asked (via email) as to how to effectively apply service packs and hotfixes to a large number of departmental systems. Kunz raised this issue in the MicroNet Group and they came up with the following three ideas:

- Use disk-imaging to roll out operating systems. The disadvantage of course is standardizing on the disk image and all applications. Probably not viable for the number of systems you have (and their diversity).

- Have your users use the Microsoft Baseline Security Analyzer. This is documented/linked-to on the web pages at www.ait.iastate.edu/win2000/admin in the "Security" section. The disadvantage is that while this is an "easy to use tool", the user must still "use it" (and they must have "Administrator" privs on the system they are running it on). Wayne Hauber (AIT) pointed out that if you are logged in with an account that has administrator privs on all systems you maintain, you can run this analysis tool remotely.

- Use the "Federated Server" concept from Microsoft to deposit "approved" hotpatches on, then point all your clients to that server and tell them "install any hotpatches from this server automatically without question". Supposedly you test them first, put them on the server, and they are automatically rolled out. The disadvantage here is that you probably need to test them on all hardware configurations or a hotfix could blow a system.

Nobody else at this WinAdmin meeting had any better ideas.

While talking about ways of making systems secure, Wayne Hauber commented that we are seeing a good number of campus systems being infected with "backdoor" products. The systems generally have file-transfer servers placed on them to distribute movies, music, software, etc. Concern was raised at the meeting that Windows XP systems were distributed "stock" from Microsoft with an "Administrator" account on them with no password. The worry was that this was a large security hole used to gain access to systems. It turns out this is only partly true. An Administrator account with a blank password can only be used at the console (not via remote login). See the following for more information:

http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/professional.asp

In the section "Blank Password Restriction" it states:

> To protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network, or for any other logon activity except at the main physical console logon screen. For example, you cannot use the secondary logon service (RunAs) to start a program as a local user with a blank password.
>
> Assigning a password to a local account removes the restriction that prevents logging on over a network. It also permits that account to access any resources it is authorized to access, even over a network connection.

[Thanks to Mike Long (CARD) for providing this URL and info]

Open Discussion

(No time available)

Meeting Adjourned (about 10:05)

Next meeting is October 11.