Windows Administrators Meeting
April 12, 2002
Minutes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

(none)

Windows 2000 Enterprise Infrastructure Progress (Kunz)

Password-Synch

This is the password synchronization from Windows up to Acropolis NetID. The software is tested and installed on the production domain controllers. It is not activated yet because a security issued was discovered during testing that requires the "pre-population" of all NetIDs into Active Directory for those users who have not changed their password since April 2000.

The problem is best explained by example. Suppose the Acropolis NetID "root" had never had the password changed since April 2000 (I assure you – this is NOT the case, but it makes a good example). It would never have been populated to Active Directory. Next, assume we activate the password synchronization up to Acropolis. Finally, suppose a Windows OU administrator decides to create an account in their OU named "root" (they can – remember – it has not been populated to Active Directory). The password-synch process pushes the password up to the ISU NetID, resetting the password for "root" up above.

The solution is to "pre-populate" Active Directory with ALL NetIDs from above.

NetID Pre-Population

In order to pre-populate NetIDs from Acropolis that have not changed their password, we sent down a "password change" command through the Account-Synch interface (in place since April 2000) with a "random character" password. A "random character" password had to be used since Kerberos has encrypted the original and it cannot be recovered to use the actual password for the NetID. This username now cannot be created by an OU admin (since it already exists somewhere else in the domain) and the "password change" security issue is resolved.

Note, however, the passwords are now "out of synch". This state can be detected on the user object with "Active Directory Users and Computers" by looking at the "Description" field for the user. It will be "Change password to use". So, the user has to do the same thing they always had to do in order to "activate" their Windows 2000 account. They need to change their password for their ISU NetID (which then pushes down a password to Windows they know). When the password is finally changed for the user the "Description" will become the proper name (first-name last-name) for the user (as on all other user objects pushed down with a password change).

There are benefits in the system for an OU admin's support of their faculty/staff. AFTER the faculty/staff users are placed in their proper OUs (which some of you may administer) the OU admins can "set" the password for those users. This sets the password in both Windows and Acropolis systems. In effect, your "administrative" control has now been extended. Your staff does not have to contact Durham to get a password reset – you can do it for them.

OU population

The long-promised action of moving user objects to their proper containers will happen as soon as the Password-Synch and NetID Pre-Population is complete. Close coordination will be done with the OU administrators.

Enforced Conventions

Kunz commended all OU admins on following the "enforced conventions" on usernames created in OUs (specifically, a "!" – sometimes called a "bang" - in front of usernames that do not exist in Acropolis). Scripts are being developed that will perform a nightly matchup of all "non-bang" usernames with NetIDs and send email to the OU admin on discrepancies found.

NAI Presentation (Dennis Engholm and Barbara Borrowman)

Barbara Borrowman and Michael Knapp, Systems Engineer (both from NAI) gave a presentation on McAfee "Desktop Firewall" and "ThreatScan" products.

Desktop Firewall

http://www.mcafeeb2b.com/products/desktop-firewall/default.asp

The ePolicy Orchestrator ("ePO") desktop management solution already exists.
NAI's existing PgP desktop has been incorporated into ePO.
Key to success of personal firewalls in a managed environment is easy installation, policy changes, maintenance, and reporting. ePO can be used to set policies from a central location for their new "Desktop Firewall" product.
"Learn mode" can be used on server setup to establish a base policy on the client systems.
"Police mode" (strict enforcement) and "warn mode" (warnings only) can be set on client systems.
Can merge local and server rules so users can add their own rule exceptions.
Can say which applications can use which ports. Example: RealAudio cannot use port 80.
Can apply rules based on individual machine.
ePO will do reporting on deployment and what is going on at the clients.
Rudimentary reporting on what software is installed on their systems available.
Includes Intrusion Detection
One large university site is installing this product on all servers to report on suspicious activity.
Various alert options available (email, pop-up notification, etc).
Will block based on both mac and IP addresses.
Administrative: Can hide firewall icon, allow user override control at desktop.
Reporting examples: Top ten attack targets. Can look at where attacks are coming from and going to. Can create custom reports via Crystal Reports or access database via ODBC.

ThreatScan

http://www.mcafeeb2b.com/products/threatscan/default.asp
Can set node on network segment to scan for devices and analyze. Will attempt to figure out operating system and services based on network responses.

Question about pushing down Microsoft Hot Fixes: Next version of ePO will make that easy to do.

Question about underlying security: Uses PGP keys and encrypted data streams.

Can give a list of systems that have IIS that are not patched properly. Can get a list of infected systems. Will not automatically apply patches or fix problems (a "best practices" concern).

Question about people moving between locations: Either have one enterprise server or decide where "home" is. Laptops with DHCP: ePO SID on system means it doesn't care what network interface is being used when talking to server.

When server is set up the agent is created with key to talk to it. Need to have admin privs to install agent on client. Can examine client software (at the client) to see what server the agent is talking to (when worried about clients installed that were not created by you).

Question on memory and hard drive space: Disk space on each client: 14 MB for VirusScan, 2 MB for ePO agent, 12 MB for Desktop Firewall. Low memory usage. More information regarding the combined product's footprint will be forwarded through Barbara Borrowman.

ISU currently licensed: (Active Virus Defense)
- VirusScan
- Virex (Macintosh)
- NetShield
- GroupShield
- WebShield
- ePolicy Orchestrator (For institutionally owned PC's. Not licensed for faculty, staff, and student personally owned machines)

New products ("Desktop Firewall" and "ThreatScan") not covered by current license.

Send email to Dennis Engholm (dennis@iastate.edu) if you are interested in participating in an enterprise approach.

Prepare for the Next Meeting!
LANMAN and NTLM Authentication Concerns (Kunz)

[The following is a reprint from the minutes for the March 8, 2002 WinAdmin meeting minutes. We will pick this issue up at the NEXT meeting. Please review and examine if this could affect your area.]

Kunz talked about the problem with older authentication/encryption protocols being used in the Windows 2000 root domain. "Back level" 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

Meeting Adjourned (about 10:30)

Next Windows Administrator meeting is April 26.