Windows Administrators Meeting
March 14, 2008
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- The “NetID Suspend” process ran Monday, March 10. This process suspends (at the Enterprise level) NetIDs for sponsored accounts that are not renewed or NetIDs for people no longer eligible for an account (graduated, left, etc.). See Section 7 (“Suspension of Accounts”) in “The Care and Feeding of Iowa State Net-IDs” document at http://www.ait.iastate.edu/pubs/ggs317/ggs317.pdf

IT Admin Administration Accounts [Kunz]

Steve Kunz (ITS) talked about problems the Windows Enterprise Admins are having contacting college/departmental OU admins because of the use of “anonymous head bang-accounts”. Kunz commented that this is the result of many OU admins correctly following past advice to not use a normal (personal) Net-ID for powerful OU administrative functions. Instead, admins should create a second account and use it only for administrative purposes when needed. However, what is happening in many cases is an OU admin creates an account such as “! OUAdmin” which has no indication as to who is using it and it cannot be used for email. As a result, many times contact with the OU admin involves scanning the most recent email sent to the Enterprise Domain Admins from admins for that OU and assuming they are the person who needs to be contacted. Often this is not the case, causing delays in resolving problems.

Two solutions were suggested in the meeting. Kunz recommended some time back that the “powerful OU admin account” be the personal Net-ID with a “!” in front of it (a “bang” account). By removing the “!” email could be sent to the real Net-ID. A second solution (used by areas in the College of Engineering) is to apply for a formal “administrative” Net-ID through the Solution Center for each IT OU admin. This Net-ID can be mailed to, with mail-forwarding set up to the “personal Net-ID” for the person. Either solution is acceptable to the Enterprise Domain Admins.

OU admins are reminded you should NEVER use a “common account” shared by multiple OU admins (each should have their own). This practice removes accountability and opens the door to several bad security practices (“we can’t change the password because too many people use it”).

All OU administrators are encouraged to correct any “non-mailable” Windows user accounts that are used for OU administration purposes to use one of the two techniques mentioned above.

LDAP Simple Binds [Kunz]

Steve Kunz [ITS] reviewed the progress being made on the LDAPS project on the Enterprise Active Directory domain. ITS continues to contact system admins that are doing “LDAP simple binds” to Active Directory.

A tentative date of **May 13, 2008** (Tuesday) has been set for shutting off “LDAP Simple Binds” to the Windows Domain Controllers. This date is following final exams for spring semester and prior to the start of the summer session.

Kunz outlined the Enterprise domain policy that will change on that day as follows:

Default Domain Policy

```
Computer Configuration
  Windows Settings
    Security Settings
      Local Policies
        Security Options
          Domain Controller: LDAP server signing requirements
            (Define: Require signing)
```

See KB823659 (http://support.microsoft.com/kb/823659) for more details on how this change will affect systems contacting the domain. Look in the “Security Settings” section, item 2 (“Domain Controller: LDAP server signing requirements”) portion of the document.

In general, modern “domain member” Windows systems will NOT be affected by this change (they use GSSAPI with Kerberos-5 for secure LDAP binding). However, some “third-party” software (Windows, UNIX, Macintosh, etc) that is not written in a secure fashion (able to utilize digitally signed connections) or is not properly configured to utilize digitally signed connections will cease to function on May 13.

Status Report on Kerberos-4 Demise [Kunz]

Steve Kunz [ITS] gave a status report on the demise of the Kerberos-4 authentication protocol supported by ITS. A tentative date **May 15, 2008** (Thursday) is planned for ITS shutting down the Kerberos-4 protocol. This date is following final exams for spring semester and prior to the start of the summer session.

One of the ITS services requiring upgrading is the Scout Server (also acting as the web-server for www.sitelicensed.iastate.edu). This service will probably be upgraded prior to the week of May 12 to avoid changing too many things at the same time. Watch the WinAdmin and CCSG mailing lists for more announcements. After the Scout Server upgrade only the latest version of the Windows Scout clients will work to install software using Scout.

ListSync for Other UNIX Lists [Kunz]

Steve Kunz [ITS] discussed a request (from the College of Engineering) to synchronize “non-official-university” UNIX lists (“moira lists”) to Windows. This sync would be performed in a similar fashion to the college, major, department, and class lists being done now. ITS staff have analyzed the work required and come up with a tentative plan. It is anticipated a new selection option will be available within the list management functions to ASW to allow “synchronization with Windows AD”. Several issues need to be addressed first:

Namespace collisions: Creation of a “UNIX list” must result in a new unique name for the same “Windows group name”. Current plans are for the Windows domain process to see if a security group by the new name exists anywhere within the domain for creation/medication/deletion. If it does exist and exists outside the “AutoList” OU structure, the synchronization request will be rejected and email will be sent to the NetID of the person attempting to create the list.

Hidden membership: It is anticipated the hidden membership flags on the UNIX list can be honored in Windows similar to “hidden membership” on class-lists. However, membership of a hidden private list will not be viewable within Windows (you will have to view the membership in UNIX). The name of the security group can still be viewed and it can be used for access control (just like class-lists).

Nested lists/groups: While untested, support should be there for “nested lists/groups” (a group composed of other groups). The “leaf groups” will have to exist first.

Ownership: Since the AutoList security groups are owned by the “Enterprise domain” (and managed by the sync process) changes to the group membership (or deleting the groups) cannot be done within “Windows Active Directory Users and Computers”. As with all other synch’d lists/groups, they are mastered at the Enterprise (UNIX) level.

A good discussion was provided on the above design by those in attendance. John Dickerson (ENGR) agreed to work with Kunz/Hascall on mockups of the above design to assure that their needs are met. Hopefully this and other feedback will result in a design of benefit to all. If you have comments/concerns/questions send them to Steve Kunz (skunz@iastate.edu).

Open Discussion

Unfortunately little time was left for “open discussion”.

Meeting Adjourned (10:05)

Next meeting is scheduled for April 11.