Windows Administrators Meeting
October 10, 2008 [Minor correction 10/13/08]
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- ITS is currently planning to upgrade the four Windows Enterprise Domain controllers to Windows Server 2008 on new hardware next summer. The last DC upgrade occurred during the summer of 2004. We anticipate upgrading one DC at a time, over a period of several weeks, starting after the spring session and completing by August 1.
- A new version of the McAfee ePO server is being rolled out (watch for announcements on the mailing lists). Two other new products from McAfee are also of interest. McAfee AntiSpyware 8.7 (an add-on to McAfee AntiVirus 8.5i) is available via ScoutKit or www.sitelicensed.iastate.edu. McAfee is also preparing McAfee AntiVirus 8.7i for release toward the end of the year. The new version will apparently do heuristics checking on local system activity and check online back to McAfee to see if the questionable program matches any new virus-DAT signatures. This method of checking will be more "up-to-the-minute current" than the updates from the last daily DAT update. Current viruses are becoming more and more dynamic in nature.

Proposed Changes for PubCookie Services -- Steve Kunz [ITSYS]

Kunz discussed changes proposed by ITS for off-campus systems using PubCookie services. John Hascall [ITSYS] sent the following message on October 6 to server admins who had registered to use PubCookies:

> Despite attempts at education, the number of members of the ISU community falling for "spear phishing" schemes shows no sign of abating. Typically, these stolen passwords are used to login to Webmail and send large amounts of spam email. Often, this causes the blacklisting of ISU mail servers, resulting in email difficulties for all of us.
>
> One step we would like to take in combating this problem is to limit the lifetime of sessions handed out by the pubcookie servers (https://weblogin.iastate.edu). Our initial thought was to limit them to 24 hours IF the client was not on-campus (presently they can select up to 30 days).
>
> We would very much like to hear if this would present a problem for you services and/or users (or if you think it is a good thing).

If you have an opinion on this issue you can send your email feedback to John Hascall at john@iastate.edu.

Discussion during the meeting indicated overall approval of the change. It was asked how this would correct the problem, since all the people using the compromised account would need to do is re-login once a day. Wayne Hauber [ITSEC] indicated that once a compromised account is detected the password is reset. Right now,

however, a reset password does not limit the lifetime of a PubCookie 30-day credential, so spamming can continue after the password is reset. Some people commented that the need for any pubcookie lifetimes over 24 hours (on or off campus) was questionable. This was discussed within ITS, but it was felt there were still on-campus uses for longer lifetimes.

User Container Renames -- Steve Kunz [ITSYS]

Kunz asked if the date of October 20 would be acceptable for the user container renames discussed in the last meeting (see "User Container Renames" in the September 2008 WinAdmin meeting notes at: http://tech.ait.iastate.edu/win2000/admin/WinAdmin.2008.09.12.pdf) and on the mailing lists. Everyone at the meeting felt the October 20 date was acceptable. Kunz will proceed with another announcement prior to 20th and then correct the container names over a few days, announcing when the renames are completed.

Darin Dugan [C EXT] asked if it would be possible to rename bang-account containers in addition to normal NetID-based containers. Kunz said "Yes – upon request by the OU admin for that OU".

ListSync of User Requested Lists -- Steve Kunz [ITSYS]

ITS is in public testing of list synchronization of user-requested moira lists as Windows Global Security Groups. The ListSync process can now handle "lists-of-lists" (including a list composed of private lists and official university lists). The only members pushed down to Active Directory are "users" (NetIDs) and other lists. Custom strings (such as external email addresses) are not pushed down (since they have no meaning as Windows security group members).

Kunz is soliciting a few more people who would be willing to help test this new facility. If you are interested in testing, send email to skunz@iastate.edu. ITS can enable selected individuals to use the new "Windows" checkbox on the list functions in ASW (see doc below). Feedback on the functionality of the facility and the clarity of the document will be needed.

A "third draft" document containing full details is available here:
http://tech.ait.iastate.edu/win2000/admin/ListSyncUserReq.pdf
Please note this document is still under construction and there may be changes prior to production release of this facility.

One comment made during the discussion was that a better word than "Windows" might be chosen for the checkbox to cause synchronization. "AD-Synch" was suggested. This idea will be passed along.

Open Discussion

During the McAfee announcements it was asked if it would be possible to bring back McAfee representatives to have a presentation on the new products and their features. This idea will be passed along to Dan Carlile [ITCSV] and Jeff Balvanz [ITCSV].

[This item corrected with proper product description 10/13/08 -- SLK] Jim Wellman [AER E] asked if anyone else was having problems with "Acrobat Professional v9 for Windows" and roaming profiles. Apparently some saved settings/paths are not handled correctly when roaming profile storage is saved/retrieved. Nobody else in the meeting was dealing with the same issue.

John Dickerson [ECSS] said they were having success with PAM access in Linux using Enterprise Domain security groups. They are using a "PAM script" that can check if the user is member of a list/group. John commented that this technique may no longer be needed with the new "user requested ListSync" facility.

The question was asked if the Enterprise Domain would support the new "Group Policy Preferences" available on Windows Server 2008, Windows Vista, and Windows XP systems (hotfixes are required in some instances to support this new facility). Kunz said that if Microsoft required a schema update to use this facility ITS will research and apply it. Multiple groups expressed an interest in this extension.

Jim Wellman [AER E] said that people should be aware that the Dell web site for ISU has wrong pricing information (higher than the actual value under the ISU agreement with Dell). Jim has found he has to config systems using the web site and then pass the configs by a Dell rep, who would correct the prices to the lower values.

Frank Poduska [ITCSV] reminded everyone that the "account suspension" processing will begin soon. Emails will begin going out for renewal reminders.

Steve Kunz [ITSYS] asked what type of personal firewalls people were using. Kunz had a long positive experience with ISS "BlackIce", but that product is now "end of life" after IBM bought ISS. Kunz and Pruski are currently looking at products like Comodo, Outpost, Online Armor, ZoneAlarm, and Sunbelt. [Note: This question does imply in any way ITS is looking at site-licensing such a product. Kunz is just interested in what others are using to purchase a product for his use]. Apparently very few people install personal firewalls (using only the built-in Windows XP/Vista firewall).

Meeting Adjourned (10:15)

Next meeting is scheduled for November 14.