Windows Administrators Meeting

July 26, 2002
Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

Updated Win2000 Web Docs

Kunz announced he had put some work in on three documents on the AIT Windows 2000 web site. Documents updated are as follows:

"Enterprise Design Summary"
http://www.ait.iastate.edu/win2000/admin/design.summary.pdf

"OU User Placement Logic"
http://www.ait.iastate.edu/win2000/admin/OUUserLogic.pdf

"Current Status"
http://www.ait.iastate.edu/win2000/admin/current.status.pdf

New OU User Drop Automation Installed

Kunz announced that work was finished on the account synchronization process so that newly created faculty/staff users are automatically dropped into their proper OU (based on official university college/department names). This action only happens when an OU is set up for the department and the appropriate "Users" container exists (see the "OU User Placement Logic" document above). The updated feature was installed July 25, 2002.

WINS Server Upgrade

Kunz and Hauber announced that the current WINS server operating systems will be upgraded from "Windows NT4 Server" to "Windows 2000 Server" during August (Aug 5-16). During that time WINS services off both primary and secondary WINS addresses (129.186.142.189 and 129.196.142.179) will be available except for brief early-morning outages (7:00-7:30 AM) when we cut over to upgraded systems. Windows client systems will need NOT changes in WINS configuration (the IP addresses will remain the same). The WINS databases WILL be flushed as new systems are brought in, but campus Windows systems should re-register themselves automatically.

A more detailed email announcement on "what" happens "when" has been emailed the CCSG and Windows Administrators lists with the subject line

"Campus WINS Server Upgrade Schedule". Refer to that email for complete details.

PswdUtil and Domain Password Age Setting (Kunz)

Work on the new PswdUtil command is complete. This command may be used by OU admins to enforce some kind of password change policy on faculty/staff within their OU (either a list of specific usernames can be provided or the name of an OU container or Windows 2000 group). Password age policies enforced by PswdUtil must by nature be MORE restrictive than the default domain policy (see below).

There was little comment about the new facility except for one email question. The question was "if one OU admin chooses one password age policy and an OU admin nested within the first OU chooses another age policy, which one takes effect for the users of the nested OU?" The answer is "the most restrictive policy". If the outer OU choose 30 days and the inner OU chooses 7 days, then the inner-OU users have a 7-day expiration and everyone else has 30 days (the desired effect). However, if the outer-OU admin chooses 7 days and the inner-OU admins chooses 30 days, everyone (including the inner-OU users) gets 7 days. There are two ways to solve this (both involving cooperation by the outer-OU admin). First, the outer-OU admin can configure multiple PswdUtil runs selecting all OUs EXCEPT the inner-OU. This would require careful analysis of where all the user objects reside so that all are covered (except for the one inner-OU). Second, the PswdUtil program could be modified to have an "exception" parm (to exclude certain users, OUs, etc) for a more encompassing run. Kunz (the author of the PswdUtil program) opted for the "first choice" for now (but will be open to mods if this proves too burdensome for OU admins).

Discussion ended on the default password expiration period for our domain. The value is currently 42 days (the Microsoft default). It was suggested at the last meeting a better domain password expiration period would be 180 days. OU admins can use the new pswdutil command to enforce shorter periods of time if they wish.

The value of 180 days was discussed and everyone in attendance felt the value was appropriate. Barring significant opposition from non-attendees reading these minutes, the default password expiration value will change from 42 to 180 days. The date for this change will be set at the next Windows Administrators meeting.

Remember, this change will only affect those accounts created without the "Password never expires" attribute set. Normal ISU Net-IDs will not be affected (UNLESS an OU admin sets the "User must change password at next login" flag either manually or with the new pswdutil command as noted above).

Windows 2000 – DFS (Kunz)

Kunz and Al Day (AIT) did considerable “Windows 2000 Test Lab Work” for support of DFS file sharing at the domain level for departmental admins. Kunz presented a long “white board short course” on how DFS works. The main thrust of DFS is to present a “virtual tree structure” on top of classic Windows network file shares to make it easier for users to find folders that may be in multiple replicas across the network.

As an example, assume a copy of an AIT departmental folder called “Docs” located on three replica servers should be accessed with \\iastate.edu\AIT\Docs once a “domain DFS root” is brought up with that name. Under the plan, the DFS root (for “AIT” and again for each department that chooses to participate in DFS) would be established on one (or more) departmental Windows 2000 servers. Links into the DFS namespace (the “shares”) could be maintained by the departmental admins, with all new links and folder contents maintained by the department.

There are two main things only a Windows domain administrator can do. First, the creation of the “domain DFS root” for each department must be created at the domain (“iastate.edu”) level. The only information needed by the domain admin is the name of the departmental DFS server (not the link-node servers where the files actually live). A DFS control folder (named for the short abbreviation of the department) must exist on this system and be shared. It is here DFS places all the control information for the DFS virtual share. The second item that only the enterprise admin can control is any “replication”. While a departmental admin can create links for the “replication locations”, the actual replication setup can only be done at the enterprise level. This (poor Microsoft) design is due to the fact that the replication functions are under the same security control as the Active Directory replication functions. There is no “replication granularity” present at the current time (other than “domain only”).

In the end once the DFS share (and any replications) are set up, all file management functions are under the control of departmental admins (including access rights on all shared files).

Greg Wilson (Foundation) commented that he has been using DFS for some time now and found there are times when Knowledge Base articles need to be referred to prevent “replication lockups” and other problems. All is not quite “perfect” yet in this release of DFS. Greg also commented that the underlying shares need not reside on Windows 2000 Server systems. A variety of shares may be used (including Novell, SAMBA, etc). The system type offering the share, however, may affect replication.

Bill Frazier (AIT) commented that the design of AFS may not promise much in terms of load balancing among replicated links in our environment. Our initial offerings may provide more info.

AIT will be establishing the first "domain DFS root" (for \\iastate.edu\AIT) with the intent on delivering MCA software in a "secure fail over replica fashion". As progress is made AIT will announce availability.

Kunz commented that departments have the option of bringing up DFS shares on their own servers as a "standalone DFS root". Using this style (separate from the domain) the mounts would be similar to "\\AITSERV\AIT\…" with your users needing to know the name of the departmental root server. Such "standalone DFS root" servers cannot "replicate", however. Refer to existing Windows 2000 documentation on DFS for more details.

Comments on DFS and how your department may use it should be sent to Kunz (skunz@iastate.edu).

Open Discussion

Dave Orman (CNDE) asked about problems with Office XP installs. On certain systems a user was repeatedly asked to reinstall components on each launch. It was suggested by someone that this behavior may be seen with both Office 2000 and Office XP are present on the same system. DLLs and registry entries are probably shared (and in conflict) in this situation.

Meeting Adjourned (about 10:10)

Next Windows Administrator meeting is August 9.