Windows Administrators Meeting
September 14, 2012
Notes (taken by Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- WINDC5 active Aug 14

Account Sponsor in Master LDAP and AD -- [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] continued a topic from the June 2012 WinAdmin meeting dealing with being able to find the sponsor of an affiliate (sponsored) account. The master LDAP data (available at directory.iastate.edu) currently has a new attribute called "isuPersonSponsorsNetID". For all affiliate accounts this attribute currently holds the NetID of the account sponsor. To have this same sponsor data viewable in Active Directory it would be most desirable to have it present on a field viewable in Active Directory Users and Computers. The question is "Where?"

At the June meeting Kunz has talked about the AD "manager" attribute (but it is unlikely that the "manager" of an affiliate user account is always the "sponsor" of that account). The "info" attribute is another possibility (which appears in the "Notes" area on the "Telephones" tab). Neither of those seems best. Kunz suggested at this meeting that a better place for the information might be right next to where the "affiliate" tag is located – on the "description" attribute (which is shown on the "Description" field on the "General" tab in ADU&C). So, for example, if the current description is "Joe User - affiliate" if would now be "Joe User – affiliate (asponsor)". One advantage would be you could use the "advanced find" feature of ADU&C to locate all accounts a given NetID sponsors by finding the description that ends with the term "affiliate (<netid>)". People attending the WinAdmin meeting responded favorably to this suggestion.

Other ideas on an appropriate AD attribute are welcome. Either send email to Steve Kunz at skunz@iastate.edu or post to the WinAdmin list. This topic will be continued in the WinAdmin/CCSG mailing lists and at the next CCSG meeting.

New User Object Provisioning - Prevent Accidental Deletion? [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] discussed suggestion that the "Prevent object from accidental deletion" box be checked for each newly provisioned NetID-based user object in Active Directory. The advantage is that it may prevent an OU manager from accidentally deleting user objects. The disadvantage is that if this protection is set you can no longer move a user object from one OU to another without unsetting the protection, moving the user object, and remembering to reset the protection.

Kunz asked if the pain (of unsetting and resetting the protection on a move) was worth the benefit of protecting user objects from accidental deletion. The response as

the meeting was pretty much "Yes". The comment was made that every AD object an OU manager currently creates has this protection set, so people are pretty much used to it now.

Comments and feedback are welcome. Either send email to Steve Kunz at skunz@iastate.edu or post to the WinAdmin list. This topic will be continued in the WinAdmin/CCSG mailing lists and at a future CCSG meeting.

KMS and EES (Enrollment Education Solutions) [Beata Pruski - ITSYS]

Windows Server 2012 is now licensed campus-wide by the latest Microsoft licensing agreement (called "Enrollment Education Solutions", which replaces the old "Microsoft Campus Agreement" licensing). Beata Pruski [ITSYS] discussed the progress of having the ITS KMS (Key Management Server) system support activations of Windows 8, Windows Server 2008 and 2012 (and other upcoming products such as Office).

Current plans are to:

1. Virtualize the existing KMS servers, at the same time moving to a Windows Server 2012 OS.
2. Install keys for all existing OS products and Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2, and Windows Server 2012.

These plans are currently delayed because the VM infrastructure will not currently support a Windows Server 2012 OS (though work is progressing on that, too). In the meantime people can use the MAK key for Windows Server 2012 if necessary. Watch for further announcements for when the KMS servers are ready for Windows Server 2012.

The question was asked whether laptops that connect via VPN only (either on or off campus) can activate via the KMS server. The answer is "No" with the reason being this would allow home systems to be activated via KMS (in violation of licensing agreements).

Comments/questions can be sent to Beata Pruski at bapruski@iastate.edu

WINDC5 Upgrade Plans [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] discussed plans for converting WINDC5 to the first 64-bit OS domain controller in the Enterprise Domain. This will mean that WINDC5 will begin offering AD Web Services for the latest PowerShell management plugins (something people have been asking for).

The main point in delaying 64-bit domain controllers is the 32-bit Kerberos DLL library used for authenticated/encrypted account synchronization between the Windows and MIT Kerberos KDCs. Beata Pruski and Steve Kunz believe they have solved the issue with a 64-bit-to-32-bit "shim" that allows a 64-bit DLL (needed to

intercept the password changes on a 64-bit DC) to call a 32-bit Kerberos DLL library.

Current plans are to convert WINDC5 to a 64-bit OS in early January 2013 (maybe January 8, 2013). This should be a transparent change for all normal Windows AD functions. However, if you have non-Windows services that are "hard-coded" to use WINDC5 for LDAP, LDAPS, or authentication services then you should probably not use WINDC5 during the winter break period (since WINDC5 will be offline for about a day during the upgrade).

More announcements about this upgrade will be broadcast as plans firm up. If you have any comments/concerns/questions send email to Steve Kunz or Beata Pruski via its-ad-admins@iastate.edu

Open Discussion

Vince Oliver [ITSYS] talked about the conversion of OCS to Lync and indicated that this would happen "sooner rather than later". As departments are moved to Lync a client update will be required. This will either be pushed out by ITS (on supported systems) or the software installer will be available on \\software.iastate.edu (it is currently not there yet). New features will be client support on an expanded list of devices, desktop sharing, and group messages (which will be added later). There are no plans for SMS support at the current time.

The question was asked as to how to clean up an SSD (Solid State Disk) drive on a system being re-provisioned or going to surplus. Using tools like DBAN (and other utilities that do DOD wipes on physical disks) is not recommended for SSD drives. Suggestions were to zero the first few hundred tracks (the boot tracks) which would make it non-bootable but leave large portions susceptible to data-mining. One person indicated they had read an article that you should encrypt the SSD drive (scrambling the data) and then do a full-pass erase. Another comment was that using a utility from the manufacturer of the SSD to do a "self erase" might be another option. It is unknown what ISU Asset Recovery is currently doing with SSD devices.

Meeting Adjourned (10:00)

Next meeting is scheduled for October 12 (provided a sufficient agenda exists).