Windows Administrators Meeting
May 9, 2008
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Week of May 12

The format of the entire meeting was a day-by-day discussion of what would happen the week of May 12-16. Several significant IT infrastructure changes have been announced and discussed for several months and will finally happen next week. In addition, some yearly processing and normal "Microsoft Updates" will occur.

Monday, May 12

The "Annual Network Cleanup" will occur in the morning. As per the announcement in the CCSG/WinAdmin/MacOSX mailing lists on May 8:

> The annual network cleanup process is scheduled for May 12, beginning at 9 AM.
>
> All DHCP address leases in the residence halls will expire but machines will get a new lease when the address ranges are shuffled.
>
> In addition, there may be a few brief outages in NetReg, DHCP, and DNS service as the residence hall networks are reconfigured and restarted.
>
> If you have questions, contact the Solution Center by phone at 515-294-4000, email at solution@iastate.edu, or in person at 195 Durham Center.

In addition, the campus WINS servers will have all residence hall and off-campus WINS entries removed (the systems will automatically re-register). On-campus WINS entries will be retained.

Tuesday, May 13

The ITS print-server will be upgraded as part of the "Kerberos-5-only" project from 06:00-7:30 AM. Printing will not be available via the print-server for a portion of that time.

LDAP "simple binds" to the Windows Domain Controllers (WINDC1-4) will be shut off at 8:00 AM. Windows domain-member systems will not be affected unless they are running very old (or non-Microsoft) applications that perform "LDAP simple binds" (which are "clear-text password authentication). Non-Windows systems with applications doing LDAP "simple binds" will also be affected.

Microsoft Updates for May will occur in the late-afternoon. Advance notice from Microsoft indicate Microsoft Word, Publisher, and the Jet Database all have critical updates. See http://www.microsoft.com/technet/security/bulletin/ms08-may.mspx

Thursday, May 15

The Kerberos-4 authentication protocol will be shut off at 7:00 AM. At that point any kerberized applications that are attempting to get Kerberos-4 credentials or convert Kerberos-5 credentials to Kerberos-4 credentials (call the "Kerberos-5-to-4" conversion) will begin to fail. All ITS services have been converted over the past year to use Kerberos-5 credentials. Now is the time when client systems using these kerberized services must use only Kerberos-5 credentials. If you still have questions, contact the Solution Center by phone at 515-294-4000, email at solution@iastate.edu, or in person at 195 Durham Center.

Two styles of the "Kerberos Configuration Tools" for Windows systems using "Kerberos for Windows" are available. "Krb4config.exe" (v2) and "Krb4config.force.exe" are needed to disable the "Kerberos-5-to-4" conversion that is happening and provide a "bug-fixed" version of the KfW "autologon.dll" library. For more information see:
http://tech.ait.iastate.edu/win2000/admin/Announce.2008.05.08.pdf

On May 15 the stand-alone installer for KfW on www.sitelicensed.iastate.edu and the version of KfW built into the Scout 9.0 installer will be upgraded to not do the "Kerberos-5-to-4" conversion and include the "bug-fixed" version of the KfW "autologon.dll" library. New installations of Scout starting May 15 will not need to use the Krb4config tools. The version number of Scout will NOT be updated, so a Scout upgrade will not be triggered (and the version of new Scout installs will still be version 9.0). Again, existing installations should be sure and run one of the Krb4config tools.

Open Discussion

Open discussion occurred freely during the "day-by-day" item discussions. What follows are some "highlights".

Someone asked if the "Kerb4config" tools would function correctly if run as a "non-privileged" user at logon time (i.e. as a user logon script or policy). The answer was "probably not" as it replaces a protected DLL. You either need to be an administrator or use the tools as "system startup" scripts.

Steve Heideman [CHEM] commented that he found some systems in his area using an older version of the "KerbAutoLogon" facility that were still getting Kerberos-4 tickets after running the Kerb4config tool. Working with Beata Pruski [ITS] it was discovered that a past upgrade to the latest version of KfW had somehow left old registry entries that the Kerb4config tool would not change (since they should not be there in the latest version). Heideman and Pruski are still looking into this, but it does not appear to be a widespread problem.

The question was asked if the only Kerberos application on a system was Eudora Pro and only the first version of the Kerb4config tool was run (so the buggy autologon.dll KfW library was not replaced) would that system have problems starting May 15? The answer is "No", because Eudora Pro uses "native" Kerberos support, and therefore does not use the "autologon.dll" library. Since the KfW "Network Identity Manager" also does not use "autologon.dll", those two pieces (Eudora and

KfW/NIM) will not suffer for the bug in "autologon.dll". However, should any of those systems use Scout, PCLPR, kpoprelay, WinZephyr, etc. they will have to have the newer version of "autologon.dll" (i.e. one of the Kerb4config tools needs to be run).

Kunz [ITS] and Pruski [ITS] reminded people that when Eudora Pro is correctly configured to use Kerberos-5 credentials, the behavior of Eudora changes when it is started BEFORE credentials are obtained (or if the credentials are expired or destroyed with the Network Identity Manager). Previously Eudora would present a "NetID/password" prompt when it detected there were no valid credentials on startup. Under Kerberos-5 configuration (if no valid credentials are present) Eudora will show an error at the bottom of its window saying "-ERR SASL authentication abort received" from client" and "No credentials cache found (try running kinit) for pop-<n>.iastate.edu". Eudora users are reminded they should get Kerberos-5 credentials (by using the Network Identity Manager, for example) BEFORE launching Eudora Pro.

Beata Pruski [ITS] commented that a problem has been found when trying to use kpoprelay with an old version Netscape Communicator (versions 7.2) and its mail client support. This old software does not follow mail-reading standards and will not work with kpoprelay. The best fix for such systems is to use "SeaMonkey", which will use Netscape Communicator's settings for mail and "do the right thing".

Frank Poduska [ITS] told people that the Solution Center has considerable additional load for email issues surrounding the "Kerberos-4 demise" event. In general the Solution Center is asking people if they have a formal IT support group and refer them to that group (so the Solution Center does not give out conflicting advice). However, people who do not have formal support (or may be unaware they have it) are getting direct assistance. Most calls last 20-30 minutes each (or more).

Wayne Hauber [ITS] and Steve Kunz [ITS] reminded everyone that an excellent tool by John Hascall [ITS] exists on ASW to query usernames and hostnames for Kerberos-4 credential use. Login to ASW (https://asw.iastate.edu), enter the "Campus IT Admin Functions" area, and select "Check Kerberos 4 Usage". Note that a "0" is a wild-card for IP scanning. Placing a zero in the last octet allows you to see all systems in a subnet.

John Hascall [ITS] reminded everyone that people who had Kerberos-4 credentials prior to 7:00 AM on Thursday will continue to have them after 7:00 AM until they expire (after 7:00 AM you will not be able to get NEW credentials). This means some problems may not show up until the credentials expire (10 hours is a common default in KfW).

Meeting Adjourned (9:50)

Next meeting is scheduled for June 13 (maybe – watch for announcements if cancelled).