Windows Administrators Meeting
April 13, 2007
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- March 11 Daylight Saving Time wrap-up. Few problems were reported. This was a "non-event" thanks to proactive work by all IT support staff university-wide.
- MS07-17 (KB925902) was an April 3 "out of band" critical update that involved an "Animated cursor exploit". The full announcement is here: http://tech.ait.iastate.edu/win2000/admin/Announce.04.03.07.pdf

WSUS and Visual Studio 2005 SP1 [Kunz and Pruski – ITS]

Kunz and Pruski spent considerable time investigating high-load problems on the Enterprise WSUS server. After contacting some IT admins and acquiring client-side Windows Update logs, it was determined the Visual Studio 2005 Service Pack 1 was the source of the problem. This large/complex update rarely installs successful via update services. Many problems arise, such as:

- Large disk/memory requirements
- Long install time
- Hidden dialog boxes

Microsoft acknowledges these problems at http://support.microsoft.com/kb/928957. ITS changed the WSUS approval changed from "Install" to "Detect" on April 10. For the full ITS announcement see:

   http://tech.ait.iastate.edu/win2000/admin/Announce.04.10.07.pdf

WSUS and Office XP Service Pack 3 [Kunz and Pruski – ITS]

Kunz said a similar number of "large installation failures" were occurring on the WSUS server for "Office XP Service Pack 3". He asked if this were a similar issue to the Visual Studio 2005 Service Pack 1 issue and if it should be marked as "Detect only", too. General consensus was that this service pack should stay marked for "Install".

Jim Wellman [AER E] found that when Office 2003 is installed on the client and Office XP Web Components are installed, the Office XP SP3 update fails to install. The fix is to uninstall Office XP Web Components.

ITS will try to get the word out on any manual intervention that may be needed to get this update to install.

Automatic Updates and Svchost CPU Overload [Kunz – ITS]

Several people have been dealing with a bug that involves Windows Updates (thanks to the College of Engineering for raising this issue). The Svchost.exe process that

runs Windows Update will stop responding. Additionally, you may receive an access violation. This access violation stops the Server services and the Workstation service. Microsoft has been trying to correct this issue for some time. It appears no final fix has been found yet. Related Knowledge Base articles are KB916089, KB927891, KB927385.

- http://support.microsoft.com/kb/916089
- http://support.microsoft.com/kb/927891
- http://support.microsoft.com/kb/927385/en-us

OpenAFS and Temp File Pollution [Kunz and Pruski – ITS]

Kunz and Pruski spent considerable time analyzing the cause of "Temp file pollution" caused by OpenAFS. To exhibit this problem the following conditions must be met:

- OpenAFS "integrated logon" must be enabled. ("Advanced/Configure AFS Client" setting for "Obtain AFS tokens when logging into Windows" checked)
- One or more scheduled tasks must be running (any account).

Temp file pollution occurs in WINDOWS\Temp with a name of the format "n.nnnnnnnn" (such as "0.50465928") each time a scheduled task runs. See the following for the full announcement:

http://tech.ait.iastate.edu/win2000/admin/Announce.03.29.07.pdf

Unix Identity Management [Kunz – ITS]

Kunz outlined the plan to populate Active Directory with several Unix-oriented attributes. In the past queries have been made for "Services for Unix" support. New support (called "Unix Identity Management") from Microsoft replaces the old "Services for Unix" for Windows Server 2003 R2 and Longhorn. ITS is working with the College of Engineering to bring up these new features. Simpler deployment of Samba AFS file services will be the first benefit derived from the changes.

This support will need Active Directory schema updates. Once the schema updates are installed, new attributes will be loaded via the ITS AccountSync process as follows:

- uidNumber (from LDAP isuPersonUidNumber)
- gidNumber (from LDAP isuPersonGidNumber)
- unixHomeDirectory (from LDAP isuPersonHomeDirectory)
- loginShell (from LDAP isuPersonLoginShell)

Everyone should be aware that these are to be treated at "Read-only" fields, mastered at the Enterprise level just like the proper name and address fields. These fields will be re-synched on a regular basis to match the ITS UNIX values.

While a solid timeline has not been determined for when this work will be done, the schema updates will probably happen soon after the end of this semester. AccountSync changes for loading the attributes will follow soon after that. Every

attempt will be made to have these changes in by early summer. ITS hopes to upgrade the operating system on the four domain controllers from "Windows Server 2003" to "Windows Server 2003 R2" shortly after the schema updates are done. Watch for future announcements.

Open Discussion

Question: Steve Heideman [CHEM] asked if anyone was converting any labs to Windows Vista.
Answer: Al Day [ITS] said that the ITS public labs would probably remain Windows XP Pro for the immediate future since the "Kerberos Login" advanced Scout-kit would not yet work on Vista. Users are too used to not having to get credentials after they login to the desktop. Other IT admins said they were still looking at Vista but most had software issues holding back widespread usage.

Question: Chris Thach [CIRAS] asked about the availability of the Cisco VPN client for Windows Vista.
Answer: A new beta version is available for testing from Cisco. Steve Schallehn will make that available to ITS for testing.

Question: Mike Long [CARD] asked if there was any way to default the login on a Windows Vista system to local account (so you don't have to preface the username with "<machine>\").
Answer: No. Only the "Administrator" account defaults to "local system".

Question: Chris Thach [CIRAS] asked how to get the drive mappings to work on a login script on Windows Vista.
Answer: Mike Long [CARD] said the following registry entry will do the trick:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System]
"EnableLinkedConnections"=dword:00000001
```

This setting may also help situations where you are running an EXE from a network drive and it wants Admin privileges, and then you find that the EXE is suddenly cut off from its files.

Comment: Wayne Hauber [ITS] commented that McAfee had released a special DAT file to deal with current vulnerabilities. This DAT file is released as the "5008" version early today (so no "extra DAT" file is required). ePO admins are encouraged to push this out to their client systems as soon as possible.

Question: Chris Thach [CIRAS] asked about how to acquire digital certificates for an internal web site.
Answer: They can be acquired in a variety of ways. Most folks shopped around external to ISU and purchased them.

Comment: David Orman [CNDE] asked if anyone else was having problems using Windows Vista via wireless. There is apparently a "wireless broadcast flag" issue. David indicates the problem is resolved by using techniques in:

http://support.microsoft.com/kb/928233

In addition, David says the "resolution" in this article didn't help, but when he made the change under "more information" everything was fine. Specifically (from the article):

If the router or the non-Microsoft DHCP server does not support the DHCP BROADCAST flag, you can set the following registry entry as follows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{GUID}

Value name: DhcpConnForceBroadcastFlag
Value type: REG_DWORD
Value data: 0

Meeting Adjourned (10:05)

Next meeting is scheduled for May 11, 2007