IOWA STATE UNIVERSITY
IT Services Technical Notes
IT

Windows Administrators Meeting

July 8, 2011
Notes (taken by Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- **Digital Certificates for LDAPS:** Steve Kunz [ITSYS] talked about the fact that the conversion of providers for the digital certificates on the enterprise domain controllers starts on Monday, July 11, 2011. These certificates support LDAPS connections to the domain controllers. On July 11 on WINDC4 only the Thawte certificate will be replaced with an InCommon one. Certificates for WINDC1-3 will be replaced on August 8, 2011. This change may have implications for you if you needed to install Thawte public certificates in the past for some process/application. Full details are at: http://www.tech.its.iastate.edu/windows/admin/Announce.2011.05.27.pdf
- **WSUS Update Frequency:** Steve Kunz [ITSYS] and Beata Pruski [ITSYS] indicated that email discussion in the CCSG group this week caused ITS to increase the frequency that the WSUS server checks at Microsoft for new updates to distribute. Previously the WSUS server was checking only once a day (at about 4:00 PM). Because Forefront FEP virus definitions may be released up to three times a day ITS has altered the WSUS update frequency to three times a day (starting at 8:00 AM).

CyFiles Implementation [Mark Bland - ITSYS]

Mark Bland [ITSYS] talked about the implementation plans from the storage planning group on rolling out CyFiles storage for Windows home-directory and roaming-profile usage for every user in the domain. Currently every user in the domain has 5 GB (you will be able to request more) of personal storage allocated to them on a storage server, although the AD user-object attributes to use that space for home-directory and roaming-profile usage have not been set (unless an OU manager has set them for their users already to storage on a college or departmental server). Sometime prior the end of July the "new account" provisioning process will not only create the CyFiles storage for new users but will connect the home-directory to drive letter "U:" and set up the roaming profile storage to a subfolder (named ".profile") in the same home directory. Specific attributes and their settings are:

homeDrive	U:
homeDirectory	\\cyfiles.iastate.edu\< fs1>\< fs2>\<netid>
profilePath	\\cyfiles.iastate.edu\< fs1>\< fs2>\<netid>\.profile

The "<nn>" portions of the path are computed from the "uidNumber" attribute for the specific NetID/username as follows (this is a VBS snippet):

```
fs1 = int(uidNumber /32) Mod 32
fs2 = uidNumber Mod 32
```

```
if Len(fs1) < 2 then
     fs1 = "0" & fs1
end if
if Len(fs2) < 2 then
     fs2 = "0" & fs2
end if
```

A DFS link has also been created for every user in the domain pointing to their CyFiles storage using the following notation:

```
\\iastate.edu\cyfiles\<netid>
```

Using the above notation the user does not have to know the full path to their CyFile storage area.

On August 1, 2011 ITS will post-process (one time) all users in the domain to connect their home-directory and roaming-profile attributes to their existing CyFiles storage IF the “homeDirectory” and “profilePath” attributes are currently “clear” (the process will not overwrite settings already established for these values by colleges or departments). The two settings will be viewed as “independent” as follows:

- If the “homeDirectory” is set and the “profilePath” is clear, only the “profilePath” will be linked to the CyFiles storage (leaving the “set” value alone).
- If the “profilePath” is set and the “homeDirectory” is clear, only the “homeDirectory” and “homeDrive” attributes will be linked to the CyFiles storage.

People are reminded that roaming profiles are currently disabled by default domain domain policy. See the January 4, 2011 announcement at:
http://www.tech.its.iastate.edu/win2000/admin/Announce.2011.01.04.pdf
OU managers can enable roaming profiles in their area by applying group policy.
See: http://www.tech.its.iastate.edu/win2000/admin/2010.12.06.Announce.pdf

The CyFiles storage will have top-level access controlled by an “autolist” group (one created for every user in the domain). Using ASW users will be able to alter this group membership to allow others rights to the CyFiles storage.

At least two people in the meeting requested the ability to “turn off” CyFiles settings for their OU. Kunz and Bland indicated that that could be possible. Specific OUs could be excluded from the one time post process attribute settings (though the CyFiles storage would still be allocated and available for later use). More information on getting on the “don’t do my OU list” will be available later.

For questions/concerns/feedback send email to storage@iastate.edu

Secunia CSI Status Report [Darrin Fischer - ITSYS]

Darrin Fischer [ITSYS] talked about progress on the Secunia CSI project. Secunia CSI is a software update system layer on top of the existing WSUS server to provide critical software updates for non-Microsoft applications (such as Adobe Reader, Adobe Flash, Mozilla Firefox, etc.).

Secunia is configured on central WSUS server (sus.iastate.edu) using three additional client-side targeting groups (which are used to get the non-Microsoft updates in addition to the normal Microsoft updates). A GPO will be provided that includes a Secunia third party patching certificate (needed for this to work).

Currently ITS is going with the mindset that we will approve everything that Secunia finds as needing patched as long as there is a package already created and only one option for the update. Main patches currently approved are:

- Adobe Flash (ActiveX and Browser Plugin)
- Adobe Reader
- Java
- Mozilla Firefox

ITS is currently reviewing patch needs on a weekly basis and will adjust this if needed. When packages are being approved we have to block inbound port 80 on the WSUS server so stations do not get patches until properly approved (this is only for a few minutes during the patch approval process).

The ITS implementation of Secunia CSI is currently in “alpha testing” but ITS hopes to soon move into “beta” mode. Currently 116 ITS hosts are in the Secunia database. Current testing includes agent stations and stations from network appliance scans. For reporting ITS is working on a automated reporting method in which departments can get patch status reports on their specific systems.

The implementation plan is currently as follows:

- Roll out to all of our ITS internal “core plus” workstations
- Evaluate and address any issues
- Finish reporting solution
- Move into “beta” mode and start inviting smaller groups of stations from college/departments that have shown interest in beta-testing.
- Move to production mode and invite college/departments to point to the Secunia client-side targeting group and GPOs.

A question was asked about SCCM integration with Secunia CSI. Darrin responded that ITS had looked into that. Unfortunately not everybody is currently using SCCM and it was viewed as having limited benefit to the campus as a whole. It is still possible to do a manual build/push of packages built for the WSUS server via SCCM.

A question was asked about rolling back updates if they caused problems. The answer is it is unknown how that would be done (possibly a normal Windows "uninstall").

For more information you can contact Darrin Fischer [ITSYS] at dfischer@iastate.edu

User Account Provisioning [Mike Lohrbach - ITSYS]

Mike Lohrbach [ITSYS] talked about directions ITS would like to move in relation to user account provisioning. One of the first things ITS would like to do is to encourage the usage of "sponsored" accounts (sometimes called "affiliate" or "departmental" accounts) provisioned by ITS instead of using "bang-accounts" ("!<netid>) created directly by AD OU managers. We currently have over 4,700 self-provisioned bang-accounts.

There are several reasons for this change:

- Tying resources such as Exchange mailboxes, CyFiles storage, VPN services, etc. is a manual process for bang-accounts. This is automated for ITS-provisioned accounts.
- Security and accountability are in question for bang-accounts. Who created them? Are they being used anymore? How are they being used (and by who)?
- Provisioning is a problem (most never go away, generally because of the previous point)

One of the first goals ITS would like to achieve is not longer allowing "bang-accounts" to have services such as Exchange mail, CyFiles storage, etc.

ITS recognizes that several needs have to be met in the "sponsored accounts" structure, such as:

- Ability to create a "service" account that does not expire (but may have a yearly reminder mail that it exists and ITS asks that you review its purpose).
- Ability to create an account (or group of accounts) via ASW without Solution Center involvement (so it could be done after hours or on weekends).
- Longer NetIDs (greater than eight characters).
- More expiration options on accounts (short-term life, no end-of-life, currently yearly-renewal)
- Ability to apply specific services (such as Exchange mail) to specific types of accounts ("service" accounts don't get Exchange mail or CyFiles storage by default, for example).

Questions/comments/concerns can be directed to either Mike Lohrbach [ITSYS] (mlbach@iastate.edu), John Hascall [ITSYS] (john@iastate.edu), or Steve Kunz [ITSYS] (skunz@iastate.edu).

Open Discussion

No time was available for open discussion this month.

Meeting Adjourned (10:00)

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