Windows Administrators Meeting
November 12, 2010
Notes (taken by Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- WINS service virtualization (completed). Steve Kunz [ITSYS] and Beata Pruski [ITSYS] announced that the movement of the WINS service to virtualized hosts is complete. On Tuesday, October 5, 2010 the WINS-1 system was moved to a virtual host. On Tuesday, November 2, 2010 WINS-2 was moved to a virtual host. No problems were reported.

Updates

- WSUS service virtualization (in progress). Beata Pruski [ITSYS] talked about ITS moving the public WSUS server (at "sus.iastate.edu") to a virtual host. The process will involve an OS upgrade to a virtual host at the same IP address. The WSUS database will be wiped (rebuilt) as in previous upgrades. This means the initial contact by client systems to the new server will involve a WSUS exchange of information with the client on what patches are present (no action is required by the client system admins). ITS intends to do this upgrade sometime between Thankgiving and the semester break (during the time that most support staff are still on campus). An outage of the WSUS server (during the day) will be necessary. More information will be posted as the change becomes imminent.
- Domain policy change for roaming profiles. Mike Lohrbach [ITSYS] talked about continued planning to change the default Windows Enterprise Domain policy to block roaming profiles. See last month's WinAdmin meeting notes for complete details ("Discussion of Possible Domain Policy Change for Roaming Profiles") at:
  http://www.tech.its.iastate.edu/windows/admin/WinAdmin.2010.10.08.pdf
  ITS is considering January 4, 2011 as a likely date for the default domain policy change. Watch for upcoming announcements. Contact Mike Lohrbach [ITSYS] at mlbach@iastate.edu with comments/concerns.
- Possible campus border block for Windows Remote Desktop Protocol. Wayne Hauber [ITSEC] gave a status report on this change. See last month's WinAdmin meeting notes for complete details ("Discussion of Possible Campus Border Block for Windows Remote Desktop Protocol") at:
  http://www.tech.its.iastate.edu/windows/admin/WinAdmin.2010.10.08.pdf
  Wayne indicated the ITS Security Group has not had much time to pursue this project but it is still on the table. Much work related to policy, procedures, and announcements/education needs to be done before any possible date can be set. It will certainly not happen this semester or during the winter break period (when external RDP sessions may be heavily used by staff).

ASW Mail-lists as Contacts [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] gave some details on ITS work in progress to make ASW mail-lists appear in the Exchange GAL at the list-owner's discretion. Various ideas for doing this have been tried in the past and rejected. One idea was to push the list to Active Directory as a security group (by checking the ASW "Windows (AD)" box) and mail-enable the resulting security group in the AutoLists container. This plan does not work because the ASW list can contain external mail addresses (such as Live or Gmail addresses) that are not populated into the AD security group.

The best solution is to create Exchange Contacts for mail-lists via ASW management. A new "Appear in GAL" checkbox will appear on the ASW "list properties" page in the mail area that will cause the contact to be created in AD (in an "AutoLists/Contacts" container). The GAL displayname will default to the list-name but can be changed by the owner. The displayname will have a suffix of the list-owner's department (to indicate departmental ownership).

Currently the "winadmin@iastate.edu" mail-list (and a few other ITS mail-lists) have had contracts created using the code developed by Kunz. You can view the contact for the "winadmin" list in the "AutoLists/Contacts" OU. Note the single email address of "winadmin@iastate.edu". You can see the GAL entry (using the Outlook address book, for example) as "WinAdmin [ITS]".

There are two anticipated problems with this design. First, the contact may already exist in another OU by the same name (and duplicates are not allowed). Second, Exchange will not allow the same email address to exist on more than one mail-enabled object. This means the external email address cannot appear on another people/contact/public-folder object (in the proxyAddresses attribute list). If either conflict occurs the ASW "Appear in GAL" action will fail with an error message and the conflict will have to be resolved.

Work remains to be done on the ASW-to-AD interface to implement the new ASW checkbox. There is currently no planned release date. Watch for future announcements.

Jim Wellman [AER E] asked if there would be a way to limit a list so only members of the list could mail to it. This would eliminate outside spammers from emailing college lists, for example. Kunz and Lohrbach indicated they would keep it in mind and see what could be done.

Send any feedback to this project to Steve Kunz [ITSYS] at skunz@iastate.edu

Open Discussion

Chris Thach [CIRAS] said that as they deploy Windows 7 laptops to staff he has been getting reports of very long login times for domain-member systems when on off-campus networks. He asked if anyone else was seeing it and had a solution. General

discussion centered around the fact that ISU has border-blocked the Windows authentication ports (135-139, 445, 593) for several years (see http://www.tech.its.iastate.edu/windows/admin/port.blocks.pdf) and it is probably the Windows 7 system not using cached credentials until after repeated tries to get to a domain controller. In all likelihood the local security policy on the system needs to be looked at in regards to using cached credentials.

Mike Lohrbach [ITSYS] commented that ITS is licensing ForeFront (a Microsoft product for Exchange server malware/spam scanning) and Secunia (a product similar to "Windows Update" that makes sure many third party products like Flash, Java, etc. are up to date). Watch for more announcements on these products in the future.

Steve Kunz [ITSYS] asked if everyone knew about "Firesheep" (http://codebutler.com/firesheep). Firesheep is a FireFox plug-in that watches networks for authentication cookies that pass by on unencrypted (non-SSL) sessions. Firesheep lists the cookies captured and allows the user to click on any of them to connect to the service (such as Windows Live, Facebook, Twitter, Yahoo, Amazon, etc.) authenticated as that user. This plug-in is very easy to install and use. People should be very careful about using popular email and social networks in public wireless locations unless they know the entire session is SSL encrypted (and most are NOT). Gmail is one good exception in that if you check the setting "Browser connection: Always use https" you are secure from hijacking by this product.

Meeting Adjourned (10:00)

Next meeting is scheduled for December 10 (provided a sufficient agenda exists).