Windows Administrators Meeting
October 8, 2010
Notes (taken by Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- WINS service virtualization (in progress). On Tuesday, October 5, 2010 the WINS-1 system was moved to a virtual host. Prior to the move a backup of the WINS database was taken and restored once the virtual host was brought up with the original WINS-1 IP number. No problems were reported. WINS-2 will be virtualized in about three weeks (last week of October).
- WSUS service virtualization (planned). ITS has been running two WSUS servers, one for "supported services and desktops" (the "ADP WSUS server") and another for "everyone else on campus" ("sus.iastate.edu"). These two servers will be combined as one virtualized WSUS server in the future. The new configuration will support the existing target groups and "Microsoft mirror" philosophy of sus.iastate.edu, so no client changes should be necessary for systems pointing to sus.iastate.edu. More information will be posted as the change becomes imminent.
- Enterprise Domain digital certificate services. ITS is researching the needs and architecture of digital certificates services in the Windows Enterprise Domain and other platforms on campus. PKI infrastructure design at other universities is being examined. New digital certificate offerings from InCommon in combination with a Microsoft AD-integrated digital certificate server are one likely design. More information will be forthcoming in both the WinAdmin and CCSG groups as this project progresses. Comments/concerns can be directed to either Steve Kunz [ITSYS] at skunz@iastate.edu or Andy Weisskopf at amw@iastate.edu

Discussion of Possible Domain Policy Change for Roaming Profiles [Steve Kunz on behalf of Mike Lohrbach - ITSYS]

Steve Kunz [ITSYS] (for Mike Lohrbach [ITSYS]) asked for feedback on an ITS proposal to change the default Windows Enterprise domain policy in regards to roaming profile storage on systems. Currently the domain settings for roaming profiles are "undefined", meaning roaming profiles (for those users that have them configured) will be stored on each system they login to as they move around campus. Since all College of Engineering students have roaming profiles a specific group policy action is required if you do not want them stored locally in your area. These group policy settings are covered here:
http://www.tech.its.iastate.edu/win2000/admin/GPforRoamingProfiles.pdf
The proposal by ITS is to take the group policy settings in the above document and make them the default domain policy.

Discussion from meeting attendees was positive (go ahead with the default domain policy change). Josh Klesel [ENGR] commented this change probably should have been done years ago.

Current thinking is to propose the policy change to happen over semester break in January 2011. ITS will listen to feedback after this change is announced in the CCSG and WinAdmin mailing lists and announce a date if no area is severely impacted. You can supply comments/feedback to Mike Lohrback [ITSYS] at mlbach@iastate.edu or Steve Kunz [ITSYS] at skunz@iastate.edu .

Discussion of Possible Campus Border Block for Windows Remote Desktop Protocol [Steve Kunz on behalf of Wayne Hauber - ITSYS]

Steve Kunz [ITSYS] (for Wayne Hauber [ITSEC]) asked for feedback on an ITS proposal to change the campus border firewalls to block the Windows Remote Desktop Protocol port (3389) to off-campus systems. This would mean that anyone wanting to RDP in from off-campus would have to use a VPN connection (via the ITS Cisco AnyConnect server or a private VPN server). The reason for this port block is that ITS Security Group analysis has shown that one of the most common vectors for hacking into campus systems comes from off-campus probes for open RDP ports. ITS has done similar border port blocks (for the same security reasons) for Windows file-sharing ports in November 2003. See: http://www.tech.its.iastate.edu/win2000/admin/WinAdmin.11.14.03.pdf

ITS did a concept test in late summer by blocking off-campus port 3389 access to Durham and Town. The test was felt to be successful. At this time the proposal is to widen the block to all campus subnets. No proposed date is set as yet.

There are some problems related to this action relating to the usability of the Cisco AnyConnect VPN server on all hardware platforms. The Apple iPad, for example, currently does not have an AnyConnect client. Handhelds, older operating systems, or non-mainstream operating systems probably will not support AnyConnect VPN clients. Possibilities for dealing with these devices are 1) use a different RDP port than 3389 (which will not be blocked) and 2) request an exception for the IP (assuming the client device has a static IP).

Discussion by meeting attendees was positive in making the change. David Orman [CNDE] (and others) questioned why we did not block ALL ports (presumably except certain “public surface” ports such as web and email) and not trim them off piece by piece. The ITS response was simply “too disruptive to too many people” (though it would certainly be more secure).

Send feedback to this proposal to Wayne Hauber [ITSEC] at wjhauber@iastate.edu

Open Discussion

Darrin Fischer [ITSYS] asked attendees about their experiences with NATing office systems (for security). Chris Thach [CIRAS] said they experimented with it and found some application problems (TN3270, specifically) and had to back off to a non-NATed IP. Steve Kunz [ITSYS] added that systems that need remote desktop access from off-campus would be a problem as well. Josh Klesel [ENGR] said that Engineering efforts with lab systems showed network performance problems early on, but he felt that problem may be fixed now (after ITS Networking was made aware of the issue).

Meeting Adjourned (9:40)

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