

Windows Administrators Meeting

March 12, 2004

Notes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- We have a couple of on-site Microsoft product sessions coming up. Both are on March 24 as follows (you must pre-register for each event):

Microsoft Operations Manager (MOM) and Server Management

Wednesday, March 24, 11:30 AM-1:00 PM

Great Hall, Memorial Union

Pre-register at:

<http://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032247160&Culture=en-US>

Content and Document Management

Wednesday, March 24, 2:00 PM-4:00 PM

ASB 1155 (ATS)

Pre-register at:

<http://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032246744&Culture=en-US>

- The schema updates for introduction of Windows Server 2003 domain controllers and Exchange 2003 servers were successful on March 6. Vince Oliver (ATS) announced that ATS already has one Exchange 2003 server in production (a web-front-end for their Exchange system).
- The Exchange “Active Directory Connector” running on the Enterprise domain was shut down shortly before March 6. The only real implication of this is that we can no longer have Exchange 5.5 systems in the Enterprise Exchange organization.

Open Discussion

- Kunz asked about a recent change (since Tuesday, March 9) on the ATS “Outlook Web Access” for client access. Since Tuesday a message about “untrusted digital certificates” had begun popping up at login time. Following the steps to trust and save the digital certificate did not appear to make the pop-up go away on subsequent Exchange logins. Vince Olive (ATS) explained that due to a server problem they had to re-install the digital certificates in a “non-standard” way. This problem will go away soon (when ATS receives new certificates).

- Jim Wellman (AE EM) asked about a “pop-up” he was seeing with Outlook access to the ATS Exchange System. If Outlook is left running the icon in the “System Tray” occasionally produces a “balloon popup” indicating Outlook was having problems contacting WINDC2. The problem goes away on its own. Discussion by the group seemed to indicate one or two others saw this occasionally. This is probably either a network or domain controller load problem (the latter will be solved by the upcoming Windows Domain Controller upgrades).
- Kunz commented that people should look at the latest version of the Microsoft Baseline Security Analyzer (version 1.2). The latest version is better than the last and was released in February. Using the product to only do one thing – “Check for security updates” – is worth the product alone. Kunz commented that this product found updates that Windows Update did not indicate were needed (such as patches to Windows Media Player 9.0 and MSXML 3.0 SP4). This product is pointed to on the Windows Enterprise Domain web-support pages (in the “Security” section) or at the following URL:

<http://www.microsoft.com/technet/security/tools/MBSAHome.msp>

- Bill Frazier (AIT) announced that the digital certificate “Thawte” web site will be changed Sunday, March 14th. The purpose is to improve service and that the “functionality of the SPKI console” is unchanged. The SPKI console is the interface that we at ISU use for the products we purchase. Bill posted an announcement to the CCSG mail-list last Friday to this effect.

Jess Robinson (CARD) asked whether or not we can get certificates that last longer than one year. Frazier indicated to the best of his knowledge the answer is “No”.

- Chris Thach (CIRAS) asked about what ports needed to be opened for proper operation of servers behind departmental firewalls. Kunz indicated he had seen Microsoft KB articles on such lists, but that the list depends on the services offered on the server. Perhaps the best approach is to go to www.microsoft.com/support and “search the Knowledge Base” for articles, using a search like “server behind firewall” or “windows firewall ports needed”. A good starting point is “How to Configure a Firewall for Domains and Trusts” (179442). This is available at:

<http://support.microsoft.com:80/support/kb/articles/q179/4/42.asp>

- Tim Nguyen-Pham (MATH) asked if anyone else was seeing problems with started tasks on Windows systems that appeared to be hardware (not operating system) dependant. He has started tasks on imaged lab systems to clean left-over roaming profile storage. This process works on Dell Optiplex systems but does not work on Precision 350 systems. The tasks do the proper thing when started

manually (so it is not a priv problem) but will not start on their own (as a started task). Nobody else was seeing this problem. Suggestions were offered about problems with the image build in relation to the hardware.

- Steve Heideman (CHEM) asked if anyone else was seeing a problem he was having with Dell Latitude laptops used with a second monitor. Whenever he uses a tool to extend the desktop to a second monitor, the system never "forgets" that setting. The two extended screens are always active. You can no longer use the system for "screen mirror mode" (for projection display, etc) since it cannot be switched out of "extended display" mode. Using the "screen toggle" key combined with changing the "extended" mode has no effect. Has anyone else seen this? Is there a solution?
- Dave Orman (CNDE) brought up the topic of departmental Exchange servers and the offering of Exchange mailboxes to people outside the department. Orman and Kunz had been discussing (outside the meeting) ideas about how portions of attributes for a user object could be delegated to some IT admin by the user (i.e. delegation of Exchange attribute rights). Ideally a script (or ASW function) could be provided for the user. Problems surrounding this technique revolve around the fact the if the user decides to switch Exchange providers there is a certain amount of "mailbox management" that has to happen in order for there to be a smooth transition of retained mail.

The discussion eventually evolved into a discussion of roaming profiles. Kunz and others discussed an old concept of offering roaming profiles on a departmental basis based on a technique developed during the Windows Active Directory Design several years ago. In a nutshell, this technique involves setting the "roaming profile" location on every user object in the domain to something like "%PROFPATH%". If a department chose to provide roaming profiles for anyone logging into systems in their department, they would ensure every system had a system environment variable set to their departmental profile storage server. If a system did not have the "PROFPATH" environment variable set then it would silently "not do roaming profiles". The "down side" of this technique when originally tested was that some systems at the time did not "silently fail" during login if the "PROFPATH" variable was not set, creating an ugly login environment. It was decided that this technique needs another look. Kunz will try to get more complete information out on the technique for others to experiment with. Perhaps a combination of profile settings, environment variables, and login scripts will do the trick.

Meeting Adjourned (about 10:30)

Next meeting is April 9.