Windows Administrators Meeting
November 14, 2008
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- The ITS Computer Inspector is used to inspect newly-NetReg'd systems for security issues. In the past people could "bail out" of the Computer Inspector process and get on the network at NetReg time without passing all the security tests. Beginning February 2, 2009, newly registered systems in the residence halls will have to pass the Computer Inspector tests after a two week grace period. A "three strikes and you are out" policy will be enforced. Upon failing the first inspection, the person may "bail out" (and not pass inspection). An email will be sent to the user with an explanation of why the inspection failed and what remediation needs to be done. One week later they will go through the NetReg/Inspection process again. Upon failing a second time, they may again "bail out" and receive another email indicating reasons/remediation. One week later they will have to go through the NetReg/Inspection process again. This time they must pass the Computer Inspection tests to get on the network. These changes will only affect NEW residence hall systems registered after Feb 9, 2008. Previously registered systems (or non-residence hall systems) will not be affected.
- A McAfee VirusScan 8.7i is now available as a production product. The ISU configured version is now available for download at www.sitelicensed.iastate.edu. Currently only the 32-bit Windows version is available. Kunz commented that one change in this version is a "safety" on disabling the on-access scanner using the system tray icon. In the VirusScan Console, under Access Protection properties, there is a box labeled "Prevent McAfee services from being stopped". You will not be able to disable on-access scanning unless you uncheck this box first. When you uncheck this box "Disable On-Access Scan" can be selected again.
- The new ITS VPN service is available. This service enables users to have their own "private VPN IP address" (with a hostname of "<net-id>.vpn.iastate.edu"). The Cisco "AnyConnect" software is installed the first time you go to http://vpn.iastate.edu . While formal ITS documentation is not prepared yet, preliminary information from the Solution Center is available at: http://www.it.iastate.edu/vpn/windows/homepage.html
- The file servers serving out the Microsoft Campus Agreement software MCACD1 and MCACD2 will be shut down on Dec 2, 2008. The replacement system is already in place and is a single system named MCACD3. This system may be referenced directly or by using the Enterprise Domain DFS share \\iastate.edu\its\mca.

ListSync Progress on User Requested Lists -- Steve Kunz [ITSYS]

Testing of the new synchronization of user-requested lists has shown few problems. It is anticipated the facility will be opened up to the general public soon. A document containing full details is available here: http://tech.ait.iastate.edu/win2000/admin/ListSyncUserReq.pdf

Windows Server 2008 License Keys -- Steve Kunz [ITSYS] & Dan Carlile [ITCSV]

ITS and the Tech CYte has found that the Tech CYte has given out some incorrect license keys with Windows Server 2008 software purchases. "KMS" keys were given out with about 50 Windows Server 2008 purchases. The KMS keys need to be replaced with "MAK" keys (Multiple Activation Keys). Tech CYte staff will be contacting all those given the incorrect keys with a new key and instructions on how to install it on the server (a server rebuild is not required – only the configuration of a new activation key). This is important to do because the KMS key originally distributed will be revoked in the future, causing any servers using it to be de-activated. Contact the Tech CYte or Dan Carlile [ITCSV] (dcarlile@iastate.edu) if you have any questions or concerns.

Windows Server 2008 Terminal Services License Servers -- Steve Kunz [ITSYS]

Members of the Engineering "E CPE" department have inquired as to whether or not ITS would bring up a "Terminal Services License Server" for Windows Server 2008 in "domain discoverable" mode. This license server would serve the entire campus, containing "Terminal Server" license CALs for anyone bringing up Terminal Services. The installation process for any Terminal Services (2003 and 2008) would query the domain, discover the "domain discoverable" license server, and receive CALs from a general pool. The concept of a domain discoverable license server has existed even with Windows Server 2003 (it not a new required feature). The premise of the proposal was that the domain discoverable license server would be loaded with a large number of (supposedly) free "device CALs", and the service would cost very little to implement and manage (on the part of ITS). It was asserted that Terminal Services will continue to rapidly grow on campus and this should be a core infrastructure service.

During preliminary discussions it was discovered that while "Terminal Services device CALs" were "no cost" in the past, licensing changes by Microsoft mean that even device CALs are charged for. Considering the number of CALs ITS would have to purchase on behalf of the university this cost quickly exceeds tens of thousands of dollars.

Kunz asked during the meeting how many people were using Terminal Services on a Windows 2003 or Windows 2008 server. Very few people using Terminal Services and the people that were using it were purchasing their own CALs and placing them on their own license server to be used by systems in their own department/college. This same technique (used with Windows Server 2003 in the past) remains possible with Windows Server 2008.

It was commented by departmental people currently purchasing their own Terminal Services CALs that they would be very happy if ITS ran a domain discoverable Terminal Services license server and paid for all their CALs. Considering the cost of the service it appears unlikely at this time.

Disk Encryption Products – Mark Bland [ITSYS]

[Note: Mark Bland presented a more detailed presentation on these products at an ITS "Secruity SIG" meeting the following week. Some information from that meeting is included in these notes. -- SLK]

Mark Bland [ITSYS] discussed a couple of "full disk encryption" products that ITS may support in the near future. Both products are primarily targeted at laptops with sensitive information on them. A full disk encryption product makes the laptop non-bootable unless the proper password/key is provided. Moving the hard drive to another system does no good – the drive is still encrypted.

The first product Mark talked about was McAfee "Endpoint": http://www.mcafee.com/us/enterprise/products/data_loss_prevention/endpoint_encryption.html This is an "enterprise class" product that will allow multiple users (with different passwords) to unlock the system at boot time. The product connects to a central administration server (managed by ITS) to allow recovery in the case forgotten passwords, unavailable system owners, etc. A specially built bootable Windows PE CD-ROM will be required to recover lost data in the event of a corrupted drive. Endpoint will also encrypt external drives (but only on the machine they were originally encrypted on). Endpoint will be a "pay for" product, probably costing between $30-$50 per system.

A question was asked about what the policies would be if a staff person becomes unavailable (leaves the university, becomes ill, etc) and they were the only person who could unlock valuable departmental data needing to be recovered. It was agreed that some policy decisions need to be made within ITS as to who can recover the data using central administration in such cases.

The second production Mark talked about was "TrueCrypt": http://www.truecrypt.org This is a freeware product available to anyone right now. This product differs from "Endpoint" in that it functions as a single user product (only one password can unlock the system). No central administration/recovery is provided. A "data recovery" CD-ROM is generated (linked to the current password) for use in the case of hard-drive damage (to recover portions of the data). A chief drawback is that if the user forgets the decryption password the drive is lost.

Wayne Hauber [ITSEC] commented that Windows Vista Enterprise edition includes a "BitLocker" facility that can also be utilized for whole disk encryption. Vista can be configured to require either a password or a USB-key (with the decryption token on it) to boot a system. More information is available here: http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption

Watch the user groups for more announcements on support of these products in the future. Contact Mark Bland (mbland@iastate.edu) for more information.

Open Discussion

Wayne Hauber [ITSEC] had a piece of information he felt others may find useful. While working on a Vista 64-bit OS he found the DVD drive quit working. It turns out he had uninstalled "iTunes", which a removed a Windows component required for the DVD drive. Re-installing "iTunes" brought back the DVD drive.

Steve Kunz [ITSYS] mentioned that the components for Active Directory management are available for Vista from Microsoft. The package used be called the "adminpak". The new name is "RSAT", meaning "Remote Server Administration Tools" (KB941314). This package is available at:

http://www.microsoft.com/downloads/details.aspx?FamilyId=9FF6E897-23CE-4A36-B7FC-D52065DE9960&displaylang=en
After installing the package on a Vista system you must activate them with Control Panel-> Programs and Features->Turn Windows Features on or off". Check the box in front of the "Remote Server Administration Tools" area.

Jim Wellman [AER E] asked if there is a possibility that the underscore character could be allowed in "moira lists". This character was disabled in the past as it caused problems with X500 mail systems. ITS will investigate. [Info since the meeting: The underscore character is now allowed on "moira lists" -- SLK]

Darin Dugan [C EXT] asked if anyone else was running a Windows Server 2008 cluster. He was having some problems. Comments were that Engineering was a good contact.

Meeting Adjourned (10:00)

Next meeting is scheduled for December 12.