Windows Administrators Meeting
March 13, 2009
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- The account suspension process continues. Emails warning about upcoming account suspensions went out the weekend of Feb 14. Actual suspension will happen on March 23 (the Monday after spring break). A reminder to OU admins – do not simply re-enable a NetID-based suspended user in Windows. Contact the Solution Center and get the account renewed at the master level. It will be re-activated in Windows automatically.
- Several important security patches came out recently. On Feb 24 Microsoft released a critical out-of-band fix to correct problems with disabling the "AutoRun" feature. See http://support.microsoft.com/?kbid=967715 for more info. Microsoft released critical security patches for Microsoft DNS and WINS servers on March 10. Adobe released new versions of Adobe Reader to cover critical security issues. Foxit Software released a new version of the FoxIt Reader (another PDF reader) to cover the same security vulnerability the Adobe Reader had.

Windows Server 2008 DCs – Security Lockdown Issues – Steve Kunz [ITSYS]

Steve Kunz [ITSYS] addressed several points relating to the tighter security standards being implemented on Windows Server 2008 domain controllers.

Microsoft documents that Windows Server 2008 domain controllers will not be allowing older "DES" encryption algorithms and are enforcing digitally signed communications. Details on these changes are available here: http://technet.microsoft.com/en-us/library/cc731654.aspx

It appears that ITS will have to use some of the override settings to weaken the domain security in our environment. In particular, many systems in use at ISU use the old DES encryption, so the "Allow cryptography algorithms compatible with Windows NT 4.0" will probably have to be enabled. It appears existing domain policies in relationship to digitally signed communications will be honored, so no changes should be noticed here. Specifically:

- Microsoft network server: Digitally sign communications (always) – this setting is currently disabled in the Enterprise Domain
- Domain member: Digitally encrypt or sign secure channel data (always) – this setting is currently not defined in the Enterprise Domain (and the default is "enabled")

Kunz took the opportunity to remind everyone that performing "simple LDAP binds" (clear text authentication) when doing LDAP queries on the domain controllers is very much discouraged. ITS will continue to strive to disable "simple LDAP binds"

as soon as we can. Macintosh systems as Enterprise Domain members continue to be a major block in the road. However, people should still be converting old applications and installing new applications to use LDAPS (LDAP with secure binds achieve by using digital certificates) at all times.

Windows Server 2008 - Backups – Steve Kunz [ITSYS]

Steve Kunz [ITSYS] talked at length about backing up Windows Server 2008 systems. The Enterprise Administrators have been spending a lot of time researching and rehearsing domain controller and domain disaster scenarios with Windows Server 2008 domain controllers. People purchasing new hardware (or upgrading old hardware) to Windows Server 2008 should be aware that Microsoft has officially abandoned the use of tape hardware in their backup product. The product from Microsoft that ships on Windows Server 2008 is "Windows Server Backup". This product is a complete replacement for the old "NTBackup" product and it only supports "direct to disk" backups (either to a locally attached disk or a network share).

A good starting point for further reading on "Windows Server Backup" is here:
http://technet.microsoft.com/en-us/library/cc770266.aspx
Note that under "Special Considerations" it says:

> "You can no longer back up to tape. (However, support of tape storage drivers is still included in Windows Server 2008.) Windows Server Backup supports backing up to external and internal disks, DVDs, and shared folders."

Kunz described several planning scenarios that people should be aware of. For example, the new "Windows Server Backup" allows for scheduled backups to a local disk volume, but will remove that volume from the available volumes on the system (and format any destroy all contents while prepping is as a backup location). This is done at the "volume" level – not the "partition" level. As a result, if you try to schedule a backup to a local volume that has multiple partitions located on it, the entire volume (and all partitions) will be reformatted to be one single hidden "backup volume). There are "safety warnings" as you try to set up the backup.

All functions of the backup facilities can be done via a command prompt with the "wbadmin" ("Windows backup admin") command. See:
http://technet.microsoft.com/en-us/library/cc754015.aspx

Kunz asked those in attendance if anyone had addressed this issue and what techniques they are using. Darin Dugan [C EXT] indicated they were using network shared folders (the large amounts of disk space). They were managing all this with a Microsoft product called "DPM" (Datacenter Protection Manager). According to Microsoft:

> "System Center Data Protection Manager (DPM) 2007 is a server software application that enables disk-based and tape-based data protection and recovery

for computers in and across Active Directory domains. DPM performs replication, synchronization, and recovery point creation to provide reliable protection and rapid recovery of data both by system administrators and by end-users."

David Orman [CNDE] indicated he was using shared network folders and the wbadmin command to perform backups over the network.

Beata Pruski [ITSYS] indicated that ITS is evaluating non-Microsoft "tape backup" products to use for offloading backups to DLT for "rotating offsite disaster storage". These products would be used to move a copy of the disk-image backup to DLT. This DLT copy could be later moved back to a disk in the event of a multi-system/multi-disk failure. One such product tested is "Novabackup": http://us.novastor.com/products/novabackup.html
Another is "Yosemite" (recently purchased by Baracuda). Symantec's "Backup Exec" remains player in the enterprise-class Windows Server 2008 backup arena. Please note that ITS is not recommending any of these specific products – there are certainly more alternatives out there certified for Windows Server 2008.

ITS recommends that anyone planning a conversion to Windows Server 2008:

1. Understand the changes in the backup methods available and plan for extra disk space to hold the backups.
2. Research third-party software if they plan to continue tape backups.

Open Discussion

Dave Orman [CNDE] asked if there was any RAID configuration that would allow a "multiple mirror to all disks in an array" (for example, if you had four identical physical drives, could you create four identical mirrors, one on each drive). Nobody in the meeting was aware of any RAID controller that could do that.

Meeting Adjourned (10:05)

Next meeting is scheduled for April 10.