AD Policy Working Group
April 19, 2013
3110 Engineering Building II
3pm-4:30pm

Present: Donna Barrett, Billy Beaudoin, Dan Green, Julie Tilley, Dan Evans, Daniel Henninger, Tom Farwig, Joshua Gira

Guests: Debbie Carraway

Business handled outside of meetings:

- "SCCM Application Model Software Deployment Policies" approved by the committee via email on 3/11/13. Alan has been asked to make available on the website and communicate out.
- Amended the Naming Convention for Service Accounts to allow for .svc in addition to .service on 3/15/13.
- OIM request to create one additional custom attribute in Wolftech AD for University password management, to work in conjunction with the PX and lastpasswordchangeddate attributes already in place. OIT would like to implement this attribute by April 18th.
  - Attribute Information:
    - oimpasswordexpirationdate
    - OID 1.3.6.1.4.1.234.1.117
    - Syntax Unicode
    - This will be linked to the ncsuaccount class, which is the class used to designate Unity/IdM accounts.
  - Attribute Usage:
    - 1 - A calculation of PX and lastpasswordchange date will be performed to calculate the oimpasswordexpirationdate attribute.
    - 2 - Shibboleth Service provider will be querying oimpasswordexpirationdate to determine password expiration.
  - This usage will require a service account. The account being used is oit.webauth.rw.service, which is the service account created by the code for the initial attributes.

=====

Agenda:

SCCM Package Model Followup
ACTION ITEM (Billy): Need to followup with Alan/Billy regarding the dates for backrev'ing the mandatory packages (both application and package models) so they'll install while the user is still logged in and nesting all of the mandatory groups into the SS groups. Billy will need to write a script to do the group nesting. Possibly between the semesters.

Application Evaluation Deployment cycle (if deployment fails, retry at this interval) -- currently it runs once a week. We think it would be better to run it once a day.

ACTION ITEM (Billy) -- check on this. If not set this way, Committee approves the change.

ADMX Additions (Dan)
We have a request (from CNR and ECE respectively) to add the Frontmotion admx files for Firefox and the Microsoft Office 2013 admx files to the central AD store.

Office 2013: http://www.microsoft.com/en-us/download/details.aspx?id=35554
Firefox/Mozilla FrontMotion: http://www.frontmotion.com/FMFirefoxCE/download_fmfirefoxce.htm

Chrome will also be updated (http://www.chromium.org/administrators/policy-templates) but was previously approved.

Daniel H: does the FrontMotion Firefox settings indicate that its for Frontmotion only or just FireFox? Just worried it might cause confusion.

ACTION ITEM (Derek): The email out to announce this needs to explain this. If we can edit the ADMX to specify that its FrontMotion, we should do so.

Committee Approves w/ ACTION ITEMS noted above.

Windows 8 and .Net Framework (Dan)
In Windows 8 and in Windows Server 2012, the .Net Framework 3.5 is a Feature on Demand. The metadata for Features on Demand are included in Windows 8 and in Windows Server 2012. However, the binaries and other files associated with the feature are not included. When you enable the feature, Windows tries to contact Windows Update to download the missing information to install the feature. It fails.

Request is to enable policy *Computer Configuration > Administrative Templates > System > "Specify settings for optional component installation and component repair"* and select the *“Contact Windows Update directly to download repair content instead of Windows Server Update Services (WSUS)”* check box.

Once this is in place, you can enable the .NET Framework 3.5 through Control Panel. In Control

Panel, choose Programs and Features, choose Turn Windows features on or off, and then select the Microsoft .NET Framework 3.5.1 check box.

Committee Approves.
ACTION ITEM (Dan): Do it.

VOIP Service/Generic Accounts (Josh)
Brief discussion of a new pilot program CNR is working on with ComTech that involves the creation of AD generic accounts for VOIP devices.

AD Remedy Groups (Dan)
I'd like to discuss the idea that we create Remedy groups for the major AD services. I'd also recommend that we prefix them with "activedirectory_" rather than "wolftech_ad_" so we'd have groups like activedirectory_wds that folks could send driver requests to rather than using the wds mailing list. Would allow them to check on status, and we'd have a way to gauge when things are piling up. Questions could still go to the list. Would recommend changing the prefix of the current _technical and _policy groups as well. Other AD services that could benefit from this?

_imaging rather than _wds
_patching rather than _wsus

Issues w/ services should still go to the lists though or we lose community support and the onus goes to those poor two or three monitoring the queues.

One suggestion -- clean up the auto reply and make it very specific that the queue is for X not Y.

SubTopic -- Alan needs more backup on WDS service group. Josh suggests that funding may be needed for the training of those new backup.

ACTION ITEM: We need to put out a public request for additional backups from the community. We also need to formally write up a needs assessment -- showing shortcomings and pass the resources request up through the governance committees.

ACTION ITEM (Dan): Rename the existing groups, and create two new ones for _imaging and _patching.

Committee Approves above.

File and Storage Committee Request (Billy)
The File and Storage Committee requests to have the AD committees come up with a "what do

we need from file and storage systems long term".

Committee: “Not it”

Updates from the AD Community Meetings, CITD (Billy / Debbie)

People liked the way governance is working, though perhaps more advertisement of who’s on it and what they’re actually doing would be helpful for others.

Better ways telling people to find info at AD website / more organization of the data on the AD website.

More SCCM training / resources was requested.

Final Report should be sent out late Summer / Fall.

AlertUs Deployment (Dan)

Client now available, but waiting on EHPS to schedule testing.

RDP Setting Update (Billy)

Lots of people have complained about RDP sessions getting dropped when GPO updates. The following fixes that. I'd like to suggest that we set this at the domain level:

- Hive HKEY_LOCAL_MACHINE
- Key path SYSTEM\CurrentControlSet\Control\Terminal Server
- Value name fDenyTSConnections
- Value type REG_DWORD
- Value data 0x0 (0)

Both Daniel Henninger and Dan Green agreed, but Tom Farwig (who confirmed it fixed the issue on Win7) raised the following points:

- Does setting that enable RDP where policy doesn't explicitly enable or disable it? No, it doesn’t enable it -- it just changes the behavior or RDP.
- Not sure what other OSes the issue exists on, but it should only be set for those OSes. I know it affects win 7 but not XP. Only Vista (and up) are affected.

Committee needs to come to a decision.

ACTION ITEM (Billy): Put it in the Desktop level policy at the domain level.

Committee Approves.

EVERYTHING ELSE WILL BE PUNTED TO NEXT MEETING

Bitlocker Discussion (Dan)

- Do we want to all Bitlocker w/o TPM? If so we must explicitly allow and note that a usb key is required.
- TPM Options possible:
  - Just TPM
  - TPM w/ PIN
  - TPM w/ usb key
  - TPM w/ key + PIN
- Boot PIN for Laptop?
  - Not desktops as we need to be able to reboot regularly w/o having to touch.
  - Minimum pin length (4-20 chars)?
  - Allow special characters?
- Should we allow users to generate a key in addition to the automated escrow?
- Encryption level -- AES 256 bit?
- Prevent Memory Overwrite? Would increase boot speed for bitlockered drive, but at the cost of some securite. Are we that worried about the speed impact?
- Unique Organization Identifier -- need to pick one.
- Removable Drives
  - optin
  - set to force devices to be bitlockered b/f you can write to them.
  - by default, older OSes (XP) can read, but not write to.
    - not certain about Macs / Linux

- What do we want to require versus allow for options?

Questions

- If you take the HD out of a PC and add to another PC, does the Fixed drive or Removable drive policies apply?

Increase the SCCM Inventory Schedule (Dan)

The hardware inventory (which includes add/remove programs) is 5 days.
Software inventory (which is the scan for all .exe's on the box) is 7 days.

I'd like to recommend that these be increased to every 1-2 days. If there are technical reasons preventing this, I'd like it discussed for the record and if work needs to be done, tasks assigned.