AD Policy Working Group
October 18th, 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, Alan Gerber

Agenda:

Internet Explorer 10 for Win7 / Server 2008 R2 (Dan Green / Dan Evans)
Patch will only affect Windows 7 / Server 2008 R2 and the only versions you might have of IE on them are IE8 and IE9. Older versions of IE (IE6 and IE7) were never supported on these OSes. Was held back from its October release (not approved for deployment other than 'Early' groups), due to a previous request from TSS to do so, but we intend to release at the November patch cycle.

- Which applications are of concern?
  - Primarily the Portal and financial applications provided by EAS.
  - Departmental apps requiring an older version of IE.
- Who exactly is testing for issues?
  - EAS "official testing" was lost with Susie Rambeaut leaving the OIT MD Technical group. They have been working to test some things internally being able to install IE v.X+1 before it's rolled out automatically. HelpDesk is now working with EAS to do basic testing and troubleshooting issues as they arise.
- What are they testing?
  - Functionality of Portal apps/panels, primarily (CIS, Financials, HR… each group has abstracted applications under the "portal" umbrella.
- IE10 has been available for Windows 7 for at least 6 months. Why was it not already tested?
  - Resource restrictions/coordination efforts -- Susie used to proactively test without a real mandate to do so to short-circuit issues and find work-around ahead of any rollout.
  - Lack of proper rights by testers to work through all portions of all apps.
- Will we be ready to release in November patch cycle?
  - **ACTION: TSS has released their hold, so we will push in November**.

Internet Explorer 11 (Dan Green)

Windows 8.1 Update scheduled to be released to the public yesterday (and to us today). One of the key new features -- Internet Explorer 11. And Microsoft has released a toolkit for blocking IE11 on Windows 7. This means that it'll soon be available for install on Windows 7 via download (expect by end of November timeframe). Don't expect a forced upgrade like the IE10 one for a good long while. Still, means we need to be testing on it sooner rather than later. No reason to wait until IE11 is released via WSUS like we have IE10.

- Same people / tests / apps as above?
    - Shift made to move all TSS Client Services (support/technical groups) to early patch groups and to better test (informal, basic functions) wherever possible. EAS should step up for better testing.
- How do we encourage early testing?
    - **ACTION: Announce its release to the lists. Encourage then. Do not plan to hold back again and state this in the announcement.**

Windows 8.1 Discussion (Dan Green)

Concerns, plans, questions? Adoption of Windows 8 on campus (within the domain) is still tiny: 377 in total. Two-thirds of which (~230) are ITECS Public Lab workstations.

- WDS/SCCM Boot images need to be updated
    - SCCM needs CU3 to be able to use 8.1 (being tested)
- Application compatibility that might forestall rollout? AnyConnect, for example? AnyConnect v3.1.03103 confirmed to work on 8.1. AFS client? SCCM client?
- Workplace Join -- allows personal machines to partially join domain. Will we allow it? Requires an ADFS server to issue certs to the personal devices.
- Makes tying Domain account to Microsoft/SkyDrive even easier…
- "Windows Defender" now includes network behavior monitoring.
- BitLocker conversion faster -- only encrypts used space versus entire disk.
- Upgrades to Powershell v4.0.
- Enhanced Task Manager / File Explorer
- Boot directly to Desktop; Start button bring up App View; and List Desktop apps before Windows Store apps (all new options, but not defaults)
- Support for Miracast, Wifi Direct printing, better wireless management.
- Autotrigger VPN when accessing resource / app requires it.
- Note: KMS Server Update for Win8.1 -- patch needed, assigned to SHS.
- Note: New Server Manager/RSAT needs to be installed: http://www.microsoft.com/en-us/download/details.aspx?id=39296
- Note: Win8.1 ADMX for GPO client settings not yet available as a download, but can be pulled out of a client machine if needed.
- TS Licensing for 2012r2 requires an update to the TS License server
- Papercut/WolfPrint (samba driver) support - need to test - currently works with 8

Import of App-V & UE-V Group Policy ADMX templates into domain store (Alan Gerber)
Now that we're licensed for MDOP, which includes App-V and UE-V, we should get the corresponding group policy templates added to the domain to manage these features. Concerns, plans, questions?

- UEV = alternative to roaming profiles - pulls application settings and presents unified "settings" based on these settings.
- Request doesn't lead to NCSU level service -- opens the option for specific units to investigate within their limited environments.
- Infrastructure required -- file server (its a CIFS share) needed.
- UE-V 1.0: All-or-nothing -- not granular enough to specify only applications X, Y and Z. Version 2.0 is supposed to be more granular
- Where stored? Can't store on NCSU Drive -- full control (or change permissions) by the user is required.
    - CVM -- can we request that the permissions on the NCSU Drive be updated to allow its usage?
- Agent will be packaged by Alan Gerber in SCCM. Other units wanting to play with this, will have deploy that application and set a GPO to specify the settings storage location.

ACTION: Committee APPROVES and requests Domain Admins to proceed.

Committee Membership Discussions

- **Moving security member of the AD Technical Working Group over to the AD Policy Working Group (Billy)**
    - Web site needs to be updated to reflect current membership of the tech working group
    - **ACTION: Committee Approves**, but we'll need to run it by the IT Strategic Advisory Committee (our parent) to be official.

- **Libraries Membership on AD Policy Working Group (Billy)**
    - If nothing else, we need to invite Emily Lynema to start attending the meetings.
        - **ACTION: Dan Green will extend an invite**.
    - Would need to be selected by AITD committee to receive one of their 4 official / voting seats.

- **SCCM Service Group Updates (Debbie)**
    - Debbie leading an effort to formalize a support model for the SCCM services on campus. Multiple meetings have already occurred and a draft proposal has been written and is being shopped around.
        - 4 service/support groups:
            - Core (service functions)
            - App packaging
            - Patching

            - Imaging
        - Asking group member management for dedicated hours per person.
        - Have received some feedback from OIT management and will take that back to the group discussing the organizational changes for incorporation before taking to CITD meetings.
        - Will present to AD Policy prior to the CITD meetings.
    - Dan Green's Personal Note on Patching Service: created and released tutorials on the NCSU patching system (for MS patches) to AD Technical folks as well as proposed SCCM Patching Service group. Wade Cornett released all of the WSUS/SCCM patches this past cycle; while there was consulting/advising from me, I was able to step away from the day to day operations role.

Campus AntiVirus Discussions / Recent MS Announcement
Microsoft quoted as advising Windows users to use a third-party antivirus. Following this and discussion on the Security SubComm mailing list, most of the NCSU interest in MS AV appears to have waned. CHASS has dropped their plans to test ForeFront Endpoint Protection as an alternative to Trend AV. However, Microsoft is apparently back-pedaling like mad -- found this "Updated Official Statement."

AV Service Team has changed the university's alternative AV product statement (from 2009) to a more generic statement. See http://oit.ncsu.edu/antivirus/clients-alternate-approved

Work is ongoing to pick a product. OIT has stood up test environments from those who met the requirements sent to vendors and S&C will begin testing shortly.

SCCM Client PowerShell Execution (Dan Green on behalf of Michael Underwood)
Request to change the script execution policy in SCCM. In the default client settings under Computer Agent there is a Powershell Execution Policy setting. It is currently set to All Signed. This can be changed to Bypass which will cause "The Configuration Manager client bypasses the Windows PowerShell configuration on the client computer so that unsigned scripts can run." This will only affect how SCCM runs scripts. All other scripts pushed through a GPO or whatever else will still need to be signed. See: http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_ComputerAgentDeviceSettings

Request is made in response to a known bug in SCCM 2012 SP1 that has been reported to Microsoft and they are working on a fix. See: http://msitpros.com/?p=1860

The long and the short of it is this. When you import or copy and paste the script into SCCM as a detection rule it is truncating the white space. Especially the last carriage return at the end of the script. When you open my script in Powershell ISE it is 149 lines long. When you important that same script into SCCM it is only 146 lines long. When you copy the script out of SCCM and paste it into a new Powershell script and try to run the script it fails saying it is not signed.

-Dan Evans: “Approving would not grant additional privileges -- simply removes the need for packagers to switch to VBscript”
-Alan suggests that we first test in CU3 on SCCM Test Env and see if it fixes the issue.

If we wanted to then turn this security requirement back on, it would break anything published in between now and then. Solvable, but you’d need to go and reimport the policies. If few people use, not a big deal, but we can’t know that.

There are workarounds w/ vbscript calling a powershell.

ACTION: Committee asks that Alan test w/ CU3 before it makes a final decision.

Ran Out of Time -- PUNTING to Email Discussion.

Windows 8 Official Baselines Live? (Dan Green on behalf of Derek Ballard & Alan Gerber)
We’ve been running our Windows 8 machines using a security baseline we created from the official Windows 7 ones -- we have to do this for each new OS as there’s always a delay on the official baselines. Microsoft has released theirs and Derek has an update on any changes that will occur in our environment should we put them in place.