AD Policy Committee
June 17th, 2011
3110 Engineering Building II
3pm-4:30pm

Present: Dan Green, Billy Beaudoin, Joshua Gira, ~~Joey Jenkins~~, ~~Daniel Henninger~~ Alan Gerber (proxy), Wes Thibodeaux, ~~Dan Evans~~ Debbie Carraway (proxy), Tom Farwig
Guests: None.

New Business:

Request from CHASS: Any objections with adding CHASS service account to “NCSU-Read Group Memberships” Required for them to be able to read the membership of the WTMG created security groups -- they're just trying to get group breakdowns for some internal tool/ list usage. If they cannot read the WTMG groups, they'll be forced to create duplicate security groups of their own that they can read.

- Account they wish to be added is "chassquery" -- which he knows he needs to rename to “chass.query".
- **Committee Approves**, but asks that they run any enduser tools past Tim before they go live.

WSUS Patch Reports -- presentation from Dan and request for Enforced ADTK weekly nag. We need to have our OU Admins keeping a closer eye on failed patches. *Sample report appended.*

- Billy: **Request** for adding a threshold for “Needed” patches in addition to failed. Example: Machines that need over 30 patches.
- Tom: need to fix the click through to the WSUS Patch Details report.
- Proposed 5am Thursday morning (prior to Thurs patch releases).
- Once all of the above is fixed, **Committee APPROVED**.
- Potential New Enforced Report -- Computer Checkins to WSUS
    - shows computers that need to be cleaned out of AD or have issues talking to the WSUS server.
    - **Request** to auto-remove non-Windows boxes from the Checkin WSUS report.
    - Plan to wait for more laptops to be added to SCCM before implementing.
    - Dan requests that the committee members test out the report on their OUs to see how well it works for them.

SCCM Working Groups (chairs highlighted)

- Pulled together to start configuring / setting up usage of the SCCM product
    - Application Deployment - Alan Gerber, Brian Carty, Brian Fields, Dan Green, Gene Morse, Kevin Swann, Ryan Leap, **Tom Farwig**
    - Imaging - **Alan Gerber**, Brian Carty, Brian Fields, Gene Morse, Kevin Swann, Ryan Leap, Tom Farwig
    - Updates (MS and non-MS) - Alan Gerber, **Dan Green**, Kevin Swann, Tim

    Gurganus
    - Scripting / Automation - Gene Morse, John Klein, Michael Underwood, Ryan Leap
- Each subgroup will need to (in the given functionality area)
    - Determine the workflow changes needed from our current practices
    - Determine/validate/recommend the permissions the a OU-Admin will get by default
    - Determine the baselines
- https://docs.google.com/a/ncsu.edu/document/d/1BEsWwBOD7Lul4LkAlN8l3G9nte-igyhZMR5rOlhNb0s/edit?hl=en_US
- Josh: Who's building / writing the "First Steps" / "Best Practices" documention for groups to use (as they can't snoop and see / look at what others are doing.
- Dan: recommend that the working groups have some brown bag lunches after they know what they're doing.
- Josh: Do we have deadlines / timelines for rollout yet? "Not yet"
- Josh: Eventually, we need an SLA...

Outstanding Issues:

Status of User Certificates?

- Slow going. ComTech needs for new wireless auth setup. They want 802.x for the Fall semester. Security and Compliance has now stated that the certs in WolfTech will be the default PKI for campus "until a better solution is found." (so we can move forward)
- 1 cert per person. Billy created autoenroll for ComTech users to test against (in WolfTech). Once testing completed, request will come to committee to approve campus wide rollout.

New website -- has been waiting on content to be added/moved for too long. Therefore, we're assigning sections and deadlines. You're expected to complete the data migration by July 8th.

- WSUS Information -- Dan Green
- WDS Information -- Alan Gerber
- Overview / Join Us -- Josh
- Naming standards -- Billy B.
- Special Groups -- Dan Green
- Software Distribution -- Tom F.
- Software Packages -- Andrew Stein
- Scripts and Tools -- Dan / Andrew / John
- References / Architecture -- Billy
- Documentation -- everyone.

Force "unlinked GPO report" to OU Admins [Dan G.] (from August 2010)

- Allow someone to identify the exceptions; Quarterly report of these exceptions.
- We want to force it to be sent once a week. Wednesday AM.
- APPROVED. Announce and include info about problem below + the fact that we moved

the timing of the report.

- **NEVER COMPLETED**
  - **It’s a powershell report. Billy has.**
  - **Need to add the owner, creation / last mod date. Make it the “unlinked and unmod for 30 days” report.**
  - **Billy needs to give the current version to Andrew so he can add it the to WT-CRON server, and dump the results to the ADTK db.**
  - Once above, make weekly enforced ADTK report as originally planned.
  - **COMMITTEE APPROVES**.

BitLocker policy (old notes below from previous committee minutes)

- *we are updating the schema to allow a permissions change that would allow computer objection to control one of their attributes -- the one that stores TPM data. Computer can then fill the info in -- and then we can store the recovery info (escrow key/paswd for TPM chip) in AD*
  - *Requirement for BitLocker deployment / management*
  - *Already tested in WolfTest.*

REVISITING Bitlocker

- CPI doesn’t require a TPM chip in their models. Being made a requirement.
- Billy, Dan, Scott, and Josh still haven’t come together to discuss possible best practices GPOs / baselines within AD.
  - Billy needs to schedule.
- Security SubComm is still waffling on the “policy” / “requirement”
- Billy: Can we make bitlocker a requirement of a new installation process in SCCM?
  - We need to have the “how to use the escrowed key to recover data from yanked drive” documented.
  - Must be limited to machines that are on the domain (so we know we have the key escrowed), is a laptop, has a TPM chip that SCCM can turn on, and must have Windows Enterprise.
  - Should we do desktops? Publically vulnerable machines? Kiosks, etc. Servers? Business officers?
    - Make it an optin - could have a group in AD that folks can drop these desktops into that the SCCM install process looks at.
    - Alan -- why not make it optout instead -- increases impact/usage.
    - Josh: lets first get a report of desktops that would even meet the reqs.
    - Committee asks Alan to specifically address this in the Imaging SCCM WG and report back.

Working Groups Established on October 2009:

- ADToolKit (Lead: Josh Gira)
  - Daniel Henninger, Josh Gira, Dan Green, Wesley Thibodeaux
  - Nothing came of this group -- CHAIR DISSOLVED 6/17/11
    - Josh thinks we already dissolved, but now its in the minutes.

- Service Level Agreements (Lead: Josh Gira)
    - Dan Evans, Billy Beaudoin, Joey Jenkins, Josh Gira
    - Group is asked to use these notes to start planning one or multiple service level agreements for usage in the domain. At a minimum, SLAs should address rights and responsibilities of OU Admins, rights and responsibilities of Domain Administrators, and general description and procedures of the WolfTech Active Directory domain service. Group will bring SLAs back to the committee for review and discussion.
    - SLAs -- final draft been waiting on Google Shares since **October 2010**.
        - **COMMITTEE MUST REVIEW, COMMENT/CORRECT, THEN APPROVE.**

- SW Packaging and Deployment (Lead: Tom Farwig)
    - Dan Green, Dan Henninger, Billy Beaudoin, Tom Farwig, Wesley Thibodeaux
    - Group should discuss the future of SW deployment in the WolfTech AD environment -- topics of discussion should include: SW group naming conventions; changes in the hierarchal group mechanism; consolidation of software repositories; automation of sw groups, storage locations, and group policies; advertizement of available software packages; responsibilities of packagers; best practices for packaging; upgrade policies/procedures/reporting and removal of old versions. Group is recommended to invite currently active campus software packagers to the discussion as well.
    - Group met multiple times to define. Have created many suggestions. Must now:
        - **Create Formalized, Web-based Request for New Packages**
            - Should be based on the request process already defined
            - Can be used for both GP and SCCM distributions.
            - DUE: 4 weeks, tops.
            - WHO: Tom + WebDeveloper (Dan offers Dan Pisciottanno)
        - Billy: Let’s also do the voting on EX package testing as well.
        - Will need to work with SCCM packaging group once they’ve completed their initial investigations in about a month.

Followup: Billy needs to review, then make public the report from the Microsoft Evaluation of NCSUs ActiveDirectory domain.

Appendix: SAMPLE “FAILED PATCHES” REPORT

Note: You are receiving this report because of your cron settings in the WolfTech ADToolkit. To view all crons you should be receiving, please visit the WolfTech ADToolkit at http://www.wolftech.ncsu.edu/adtoolkit/

WSUS Patch Overview

This report will show you an overview of your computer's patch statuses. Which of your computers still need patches, which need to be rebooted to complete their patch installations, and which computers have errors or failed patches. It is critical that all failed patches be investigated and resolved. Keep an eye on computers that need to be rebooted -- if they're not rebooted, they're not protected -- and any computers with a large amount of patches needed.

Search Criteria:

- **OUs**: NCSU/COE/ECE
- **Status**: Failed

Results Returned:19

Computer	OU	Needed	Reboot Required	Failed
ANIAK	NCSU/COE/ECE/Research Labs/Public/Lab	1		1
arlene	NCSU/COE/ECE/Research Labs/paulf/Desktops	25	2	1
cab	NCSU/COE/ECE/Staff/Admin/Laptops	18		10
dijon	NCSU/COE/ECE/Research Labs/dschuri/Desktops	22	1	1