AD Policy Committee
December 16th, 2011
3110 Engineering Building II
3pm-4:30pm

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

Absent: Dan Evans

Guests: **Michael Underwood, Debbie Carraway, Alan Gerber**

Actions Outside Meeting:

- Added https://ssprd.acs.ncsu.edu/ to the list of Trusted Sites in the default domain IE policies – its for Singularity document imaging and is tied to the portal.
    - https://sysnews.ncsu.edu/news/4c7d355f

New Members

- Julie Tilley – CVM
- Donna Barrett -- MGT

Account Lockout Policy (request from IAM Project group via Debbie Carraway)

"Currently, the eDirectory that the MyPack portal uses is configured to lock an account out after 10 consecutive failed login attempts over an unconstrained period of time. At that point, the account is disabled for 30 minutes. Portal authentication is transitioning to Active Directory. The IAM project team working on replacing eDirectory has asked whether AD Policy would support the implementation of a similar configuration in WolfTech."

- WolfTech already has a 10 wrong logins lockout that locks you out for 15 mins. Debbie confirmed that this is fine for MyPack.

Firewalling Remote Desktop (DanG)

- Massive increase in attacks against RDP.
- Causing accounts to be locked and unusable
    - in one 24hr period, we saw 1700+ lockouts
        - computer logs are filling up with RDP rejections
    - due to the way we have Windows setup, few people noticing
        - however, as we point other services at AD for auth, those services could noticing a lot more -- MyPack, Mediasite, etc...
- Security Comm is discussing blocking at the campus gateway.
    - thought of as a best practice by many.
    - they want to try to get more details – where's it actually coming from?

    - Better data -- is it all RDP, or are we seeing other protocol attempts causing the lockouts as well?
    - VPN implementation – can it handle the increase? Mobile support? NonUnity accounts (vendors) that need access?
    - Generally, the consensus was that its something we need to do and is moving forward to work out the details.
    - Billy has a concern that adding firewall rules on the AD might hinder adoption of AD on some wild/wild west machines – faculty not wanting to deal with the extra step to talk to their machine.
    - Any special impact on VCL?
- ECE announced issue and planned firewall updates to block
    - Surprisingly, zero complaints.
    - Plenty of confusion over ComTech VPN instructions
- Should we be recommending this out to the OU Admins? What do we need in place before we do so?
    - Better VPN docs (ACTION ITEM: ECE has a sample it can share)
    - Better GPO instructions for those that wish to implement.
        - ACTION ITEM: as DanG is in the process of doing, will write out the steps an OU Admin will need to take to enforce at his OU.
    - Politics may hinder rollout in some colleges
        - Billy: could we do a default, and you have an option for a deny group for the complainers.
    - Daniel H: If only ECE and CHASS does, does it help? Attempts against other depts will still lock you out. But you do at least drop the number of target-able machines (and one hopes, the number of individual attacks).
    - Getting us to optin now, makes it easier for SecComm to push the policy through.
        - Plus, its going to take a long time -- why wait if you can start to protect your PCs now.

Update re: Domain Controller request for Env Health/Public Safety

- Still waiting on Dan Evans to coordinate meeting to iron out.
- We're hearing that the network over there may be firewalled off from campus -- if so, that's an issue. Lots of ifs, need technical details from EHPS.

Update re: Trend AntiVirus / AD Software Groups (Michael Underwood)

- What should OU Admins be doing?
    - Putting machines into EX-Trend Micro-OfficeScan-10.6
    - Do so as soon as possible. And over time, as machines are rebooted / locked out of, they'll get the newest client.
- What happens when they do this?
    - 4hrs later, machine starts to download. Once it has it, AND once no-one is logged in, it starts an uninstall of previous version and reboots. Then installs new version.

        - ECE will do so tonight.
    - Michael has checked all product codes reporting in AD and believes he has them all covered - aka, this is as tested as it going to be. Need to have folks make the move.
- ACTION ITEM: We need to send an email out to the AD list and push this recommendation. (DanG made a note to do so first week in Jan).
- ACTION ITEM: Get this group out of EX (DanG made a note to do so first week in Jan).

Update re: BitLocker Deployment (Michael Underwood / Billy)

- NCSU-OS-Windows 7 SP1 Enterprise-Bitlocker-x86/x64
    - if laptop, Dell/Lenovo, + TPM, turns on chip/Bitlocker
    - does it escrow key? yes (in AD)
    - how to encourage? force usage?
        - NO, don't, still in testing. Try it, report, before you use across your labs.
        - Billy is hoping to have a class in early 2012 to instruct folks on SCCM installs and encourage usage in this manner.
    - **SCCM install -- not if you install via PXE**
- Still need to create a domain wide (optin) GPO for enabling Bitlocker for domained machines (for turning Bitlocker on for currently installed laptops / desktops)
    - ACTION ITEM: schedule this subgroup to get together and flesh out.
- And need to look at bitlocker and removable drives at some point...

Update re: autodisabling of .admin accounts for dead UnityIDs.

- script now completed, permissions issues resolved (was preventing us from accurately identifying accounts that were already disabled).
- Sysnews post will go out next week. (ACTION ITEM - DanG)

WolfTech (ECE) Staff Rollover

For Your Information: Andrew Stein (and another WolfTech programmer) will be leaving NC State early January. This will impact WolfTech's resources -- and in turn development cycles for ADToolKit and other scripting/automation projects.

- DanG expressed the hope that Debbie's (OITs) new AD Architect position could assist with AD scripting/automations once hired.

Scheduling 2012 Meetings

- Friday 3pm still work? 3110 EB2 OK? No objections.
- ACTION ITEM: Schedule 2012 Meetings.

Firewall rules for Applications (Billy):

- **(revisiting -- TABLED during past meeting for email discussion or next Meeting)**
- When packaging applications for deployment to campus systems on Windows, the default rules are for closed, open to local subnet, and open to the world. In making a number of applications work correctly, firewall rules are being set to "open to the world"

or "*". If determining the exact hosts that need access to a port for an application, app packagers are recommended to use the follow list that corresponds to "on-campus": 152.1.0.0/16, 152.7.0.0/16, 152.14.0.0/16, 10.0.0.0/8, 172.16.0.0/12

- We need to go back and review the current status of applications. Get a list, come back to the Comm or email out for discussion.
- Then we need to express this as a packaging guideline? Or at least for NCSU level packages?
- Is there anyway to script something that checks / scans for this?
- ACTION ITEM: Someone needs to review the current versions of major apps? Billy will do some, and force some of his minions to help.

New 1.7.3 AFS client package coming soon...

- Better support for Laptops
- Better support for Windows x64
- No loopback adapter requirement