AD Policy Working Group
February 15th, 2013
3110 Engineering Building II
3pm-4:30pm

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

Absent: Julie Tilley

Guests: Debbie Carraway, Alan Gerber

Business handled outside of meetings:

- 2/12/2013 -- Committee approved creation of oneway trust between WolfTechAD and the IES domain for the purposes of migration. Trust shouldn't last longer than one year.

=====

Agenda:

Renaming administrator account (Dan)

Internal audit has asked that we rename the default local administrator account on all domain computers. We currently do this, however, they're concerned with our current choice. Many units have already overridden this settings at their OU level -- this change will not affect these groups. We need to decide on a new default name for the account, and communicate it out to the campus OU administrators.

Action Item (Dan): *Committee decided on a new name (not listed for security reasons) and requested that the domain administrators update the policies which set it. Sysnews post will be created to inform the Active Directory community.* [https://sysnews.ncsu.edu/news/51228506]

AD Audit Results

Billy, Debbie, and Dan G discussed the recent Internal Audit report. Details not listed for security reasons. **Action Item (Billy):** Can we share the report with the Policy Comm and if so, do so. (Yes, we can).

Wolftech AD Webauth Attributes Update (Debbie)

Request: Create two custom attributes in Wolftech AD. These attributes allow password management for University web applications. OIT would like to move webauth from eDir by Feb 4th.

Attribute information:
px OID 1.2.840.113556.1.8000.2554.999999.2.1
lastpasswordchangedate OID 1.2.840.113556.1.8000.2554.999999.2.2

In test we have the attributes as unicode, in production this might be a numeric/text string syntax. I would like to talk about linking it as optional to the user class.

Attribute Usage:

1- an initial "seed" script that will copy all the PX and lastpasswordchangedate data from eDirectory to AD
2- the university password change page, that will update the lastpasswordchangedate as customers renew their password.
3- the password reset help desk function which will clear the lastpasswordchangedate, thus requiring the user to perform a password change if the Shibboleth Service provider enforces password expiration.
4- the daily script that determines if the security profile (in PeopleSoft) for individuals requires a change in the PX password policy and if so- update the PX value in AD.

This usage will require a service account. In test we named the account oit.webauth.service.

Tech Committee Response and Answers:

- px - 1-5 values (maybe a better name?) - **So much different code is using these attribute names. This would be very hard to change.**
- lastpasswordchangedate - password change page (would that include password reset tool and administrative disable?) **Yes, the password change page is moving to AD as well along with the associated tools. The User Lookup Tool will be updated.**
- Prefer to use NCSU OID's - http://xteams.oit.ncsu.edu/iso/docs/dir/oids - **done. I have a block of OID's for AD attributes from Tim.**
- Add to previously used child class of user - **will be done when added**
- Not sure about using unicode. Ok if not, but prefer unicode - **unicode will be used.**
- write with current service account, read with webauth account - **done. r and rw accounts will be used.**

Policy Committee questions:

- Can these be readable? **Will be by .admin accounts, yes.**
- Will it be added to all user accounts? **No, only Unity accounts in the People OU.**
- Are these going to be mass-populated with existing e-dir values? **Yes.**
- Will this result in AD accounts being locked? **No new process for locking AD accounts will be created as a part of this move.**
- Is this going to be replaced by something in the ID Management system in time? **We'd expect these values to continue to exist and be populated, though the IDM mechanism to do so may certainly evolve.**
- Since we can't rename the "px" attribute, could we alias it to have something more readable?

- Who will have write access? **There will be a service account that will be created for this process and the domain admins.**

Committee Decision: Proceed.

SCCM Application Deployments (Alan / Billy)

With a new method of deploying software, we have a new set of policies and guidelines to set for that method:

- Naming conventions for NCSU and nonNCSU apps
  - Appearance in Admin Console
  - Appearance in Software Center
- Application Catalog metadata:
  - Verbiage of description for NCSU apps. Example from Silverlight application: "This is an EXPERIMENTAL software package provided to the entire NC State community. Silverlight is a free web-browser plug-in that enables interactive media experiences, rich business applications, and immersive mobile apps."
  - User help documentation link -- should link to vendor support site unless there's an NCSU support site for this application. Not to be used to point directly to remedy groups or support emails.
  - Custom icons -- optional
- Change application deployment evaluation cycle to something more frequent than weekly
  - Alan proposes that we change this to daily. Will assist with application deployments that need to be told to retry after a failure. If enduser removes, app will reinstall the next time this eval cycle hits. (if you want the endusers to have the option to uninstall, you should consider using SelfService instead of Mandatory assignments)
- Allow app creators to create custom global conditions (optional functionality) -- examples include 32vs64. Similar to WMI filters. Currently only SCCM admins can create. App Creators are currently limited (not all OU Admins are this). As part of getting App Creator perms, they'll be instructed to be careful w/ this ability.
- Process to elevate GCs to NCSU-level
- Allow use of supercedence & dependencies for NCSU apps -- would allow central packages for a new Java to upgrade existing installations of older Java. Decision to use will be per application.
- Install while user is logged in for NCSU apps?
  - using maintenance windows could help prevent installs in scenarios like ClassTech computers -- you'd not want an assignment at 1pm kick in at 2pm during a class (you'd use to push it to 10pm for example).
  - selfservice will ignore maintenance windows so those wanting to mix SS and mandatory could do so.
  - we need to email out to the OU admins and explain this and the benefits of maintenance windows.
- Uninstallation rules for NCSU apps

- Move/copy existing NCSU packages to the app model -- benefits our move to a supercedence model. Want to jump the EX testing as its identical to existing package. Will also try and add in missing uninstall info if possible.
- App detection rules for NCSU apps -- is it allowable to continue to adjust/add even after going production. Currently once it goes SW, we try to be hands off. (are there PCI issues with this?) Regarding quality -- perhaps not only use registry settings -- look for both registry plus files existence.

Nesting the mandatory group into the selfservice group. If mandatory, application model will gray out the “remove” option in the software center. Mostly just changes the list of apps that shows up in the Software Center. Technically, would let users on a computer that will mandatory install an app later, to install NOW. Might be useful for folks installing a new machine.

ACTION ITEM (Alan): Write up the announcement/explanation for the OU Admins, share with Committee for blessing.

Meeting adjourned at 5:05pm. The rest of the agenda will be discussed via email or at the next meeting:

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".

VOIP Service/Generic Accounts (Josh)
(details to be provided in email)

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 eskrow?
- 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.
- Removeable 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 optins?

Questions

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