# Agenda/Minutes 02/19/10

Friday, February 19, 2010
12:09 PM

**In Attendance**: Dan Green, Billy Beaudoin, Joshua Gira, Joey Jenkins, Daniel Henninger, Wes Thibodeaux, Dan Evans, Tom Farwig, Kevin Swann

1. Minutes from Previous Meeting: Approved.

2. Updates from IT Comm [Billy]:
   a. Domain Controllers and DFS servers upgraded
   b. Forest Level moved to Server 2008 R2 function level
   c. Recycle Bin in progress; coming soon.
   d. Network driver issues w/ DCs still being examined.
   e. WT-DC-00 (virtual machine) -- getting butt kicked, needs to have better resources or axed. Prefer to keep it for disaster recovery reasons. DC Admins continue to work on it.
   f. Windows 7 policies were put in place
      i. Pending changes: non-OS specific settings (cleanup) such as allowing pings globally;
      ii. Pending changes: turning off IPv6 (Win7/2008 may be seeing it and using as default -- causing issues/delays).
   g. Mac Extensions being tested in WolfTest by John Klein / Everette Allen

3. Account Attribute Priorities [Billy Beaudion]:

   Moving from ECE maintained account provisioning (based on LDAP changes) to OIT code which will use existing UnityID creation steps.

   Why important:
   a. Default paswds will be correct
   b. Earlier creation of accounts
   c. Passwd change page -- failure to update WT paswd will be major failure and force rollback [this will be an option to do this -- not an immediate effect of the scripts change]
   d. OIT HelpDesk Password Resets
   e. Able to change Sysnews Lookup AD info to point at WolfTech AD vs OIT AD.

   The following table lists the attributes that are set on Active Directory user accounts in the "People" OU:

   Active Directory Account Attributes Attribute Value

   yes distinguishedName CN=<Unity ID>,OU=People,DC=wolftech,DC=ad,DC=ncsu,DC=edu
   yes cn <Unity ID>
   yes samAccountName <Unity ID>
   maybe givenName <First Name>
   maybe sn <Last Name>
   maybe displayName User's full name from online directory
   yes userPrincipalName <Unity ID>@wolftech.ad.ncsu.edu
   no altSecurityIdentities Kerberos:<Unity ID>@EOS.NCSU.EDU
   yes userAccountControl 65536 (password never expires, account enabled)
   65538 (password never expires, account disabled)
   yes pwdLastSet -1 (Disable "user must change password at next logon)

| | | |
|---|---|---|
| yes | unicodePwd | Initial (default) Unity password |
| yes | objectclass | ['top', 'person', 'organizationalPerson', 'user'] |
| yes | gidNumber | <Unix GID Number> |
| yes | uidNumber | <Unix UID Number> |
| maybe | gecos | User's full name from online directory |
| yes | ncsuCampusID | Campus ID number for user |
| yes | ncsuAFSPath | AFS location of mount |
| yes | loginshell | Unix shell for SFU - for Unity users, usually /bin/tcsh |
| maybe | initials | User's initials |
| maybe | mail | User's e-mail address |

Committee approved the maybe's (f/lname, initials, displayName, etc) with the requirement that we'd go back and fix the perms after populating; locking down to address FERPA/privacy concerns.

Mail -- Vote was to approve [especially as we're already doing this]; do across the board, but as with the above, protect from general viewing (a la the f/lname FERPA reqs).

(question came up -- can this be multi-value in AD?)

Committee approved all required and SFU required attributes. (gid/uid/loginshell/gecos)

ncsuAttributes: Will require user class schema extension? Daniel suggests adding ncsu object class instead. Committee Approves both below; technical comm will need to address implementation options above.

-CampusID: protect who can read w/ group (need to define who -- there are scripts that need it. OU Admins? Domadmins?). Approve creation of the group -- but need to later lock down who needs access (discuss w/ IAM/Sec). Joey suggest that OU Admin needs this -- plus they already have access via Sysnews tools.

-AFSPath: Would be nice for RealmKit (linux); could be used by Windows AFS client script.

4. Software SubComm recommendations to be discussed [Tom Farwig]:
   - Remove the date string for new groups and GPOs
   - Add an optional GPO version string in place of the date string if a naming conflict exists. Date string currently takes up 8 characters, version string would be considerably less if necessary.
   - Switch to OU name first then EX/SW/FW for policy name and the group name. ex: NCSU-SW-* instead of SW-NCSU-*
   - Keep the vendor name, however we need to check the consistency of vendor names or vendor name abbreviations.
   - Remove the Freeware and Experimental OUs under software packages, and move those packages into the appropriate "<OU> Software" OUs.
   - Keep 32 and 64 bit distinctions out of the Software Group names. Use same group for both and a separate GPO with the appropriate WMI filters.
   - Use as much of the vendor software version string as possible to distinguish between one version and a patched or upgraded version. ex: Adobe Acrobat Reader 9.1.3 instead of Adobe Acrobat Reader 9.

   Committee had no objections for the above.
   We would like to see:
   1. deny groups for each SW group
   2. possibility of not having every software group being created (allowing you to choose).

   Dan Green mentioned that he has Stein working on more reports / scripts for managing SW

groups.

Next meeting: Feb 22nd: top points -- SW lifecycle / automations.

5. Funding Discussion [Billy]
    a. WDS servers (prime example): not just hardware, but PSS service call option paid by?
    b. Everyone agrees that they should be paying SOMETHING. But hand them a bill and they want specifics / to know that they're paying their fair share (AND NOTHING MORE).
    c. Kevin Swann: OIT just purchased PSS support. Details:

*As I have reported in the Wolftech AD Policy Meeting. OIT is purchasing Microsoft Technical Support calls. I said that we would be trying to purchase the TechNet libraries for each of our Windows Services team. The TechNet has the libraries that would be valuable in troubleshooting and researching the MS OS, AD, and Products. It also is supposed to provide 2 Tech Calls for business hours. We were also going to try to get 5 – 10 Tech Calls for 24 / 7 support. This all is part of OIT beginning to have more involvement, care, and support of the central AD, Wolftech.*

*Here is the follow up to date:*

*We cannot buy critical support incidents (after hours) in advance. We can only purchase that type of incident when we need to use it. The only way to get around this is to purchase into Premier Support, which starts at $37,000. They have eliminated their lower tier contract support option.*

*They only offer 5-packs of 6AM-6PM PST incidents in advance.*

*We are trying to see if there is any way to reserve a pool of money to use during the year as needed? It is unlikely that this model would work very well with our need to use the money. We were thinking of 10 after hours incidents at $515/ea, for a total of $5,150. However, it may be that we just use the Business hours packs, which would be more than we have currently. And work the xray, panic, emergency if they ever occur at the time that all hope is lost.*

*Bill Coker is working the TechNet Plus Direct subscriptions through our Microsoft Volume License Agreement. Apparently we do have access to TechNet Direct through our Microsoft Agreement. he just needs to activate it.*

*The details of that are:*

*One, the TechNet we have access to through our agreement is TechNet Software Assurance Subscription Services but we get access to it by selecting TechNet Direct Plus.*

*Second, it only allows the addition of one user although it implies many could be added. I am the one who is currently added.*
*Bill is following up with our Microsoft rep to see the next steps.*

*After we determine the TechNet final details, we will purchase the Technical Support Calls as we are allowed with in our budget. We may still purchase additional TechNet subscriptions if we cannot add more people to the agreement Bill Coker has.*

d. Need to start listing out servers, VM costs, PSS support, storage
    i. DCs, DFS, WDS, WSUS, Cert Service, Cron
    ii. Storage for above + software packages + backups
    iii. Training?
    iv. Account for FTE, if not charge
    v. CALS, software licenses, OS licenses

6. "Home Directory" attribute and OIT Storage [Billy]
    i. If we were to set, then we'd need an exceptions procedure/policy.
    ii. We're worried about effects on desktops / endusers
        1) We can't test every app
    iii. Folder Redirection?
    iv. Effects on desktops vs laptops? Onsite vs Offsite?

TABLING -- we need to get a group of those yelling the most into the same room. Plus these people need to have it set (and alt attributes) for testing.

7. INTERACTIVE [Dan Green]: PUNTED; AGAIN!
8. Best Practices for Storage [Josh]: PUNTED
9. Services -- Maintenance / Outage Timing [Daniel Henninger] PUNTED TO EMAIL

(NOTE: an out of band meeting has been scheduled for 3/12/10 to address these punted issues and other points)

Notes: changed mailing lists:

Wolftech-ad => activedirectory
Wolftech-patches => activedirectory-patches
Wolftech-policy => activedirectory-policy
Wolftech-domadmin=> activedirectory-domadmin
Wolftech-software=> activedirectory-software