AD Policy Working Group
Aug 22nd, 2014
3110 Engineering Building II
3pm-4:30pm

Voting Members: Donna Barrett, Charles Cline, Dan Green, Julie Tilley, Dan Evans, Daniel Henninger, Tom Farwig, Joshua Gira, ~~Payman Damghani~~

Ex Officio Members: Jeremy Brown, Michael Underwood, Gene Morse, Jonn Perry

Guests: Billy Beaudoin

Business handled outside of meetings:

WSUS Upgrade [Jonn Perry, 7/3/14]
On July 23st, 2014, the SCCM Patching Service Team hopes to change out the current campus Stand-alone WSUS server with a new WSUS VM running Windows Server 2012 R2 (current service in running on Windows 2008 VM).

The new server (which will reside in the NCSU/Servers/WSUS OU) has already been provisioned and patched and updated to the latest version of WSUS, version 6.

They will also update the WSUS console in Citrix.

Reason for Change
Moving the service to VM containing a supported version of OS & software.

Impact
Patching updates during the upgrade window. WSUS Patching will be temporarily unavailable, no more than 3 hours.

Change Implementers
Wade Cornett; Jonn H Perry (Backup)

Release or Deployment Plan

- [done] Copied and exported the necessary certificates from wt-wsus-00 to wt-wsus-02.
- [done] Expanded the D: drive of wt-wsus-02 from 40GB to 190GB.
- Add to VLAN vl37-dc2-6509-2.ncstate.net [NCSU].
- Move the A record for MSUPDATES.NCSU.EDU, to the new WSUS Server.

Rollback or Backout Plan

- A backup of the WSUS database will be taken prior to migration.
- The database will be restored if there are any issues and MSUPDATE.NCSU.EDU will be pointed

back to the old WSUS Server.

ACTION: Committee Approved Timing / Proposal. 7/8/14. Proposal passed to AD Tech.
UPDATE: 8/21 -- new migration date will be announced now that the issues from last attempt have been identified and resolved.

Adding service acct to "NCSU-Read Group Memberships" [Dan Green, 7/30/14]
We have a request from CALS (Jamie Dennis) for a service account to be added to "NCSU-Read Group Memberships":

“With the recent change in password policies, we removed our service account from the OU admin group and adjusted its rights accordingly. The one feature it was getting from being an OU admin that it now lacks is group membership lookup. This account is used for Symantec DLO backups. Part of that is automated user configuration within the system. This requires the account to query the AD group membership of the user logging in.“

The account in question is "CALS.DLO.service" -- it was calsservice.admin, but at the request of the AD Tech Comm, it has been changed to comply with the AD account naming convention. They have approved this request.

ACTION: Committee Approved 7/31/14. As this was already approved by AD Tech, Dan Green implemented.

Adding service acct to "NCSU-Read Group Memberships" [Dan Green, 8/6/14]
We have a request to add "CALS.crashplan.service" to the "NCSU-Read Group Memberships" security group by Jason Robinson of CALS IT.

The background is that Plan42 (vendor) setup a mini Crashplan system on a Mac Mini in Jason Robinson's office (so local, not offsite). The intention is to use this to test / plan out deployment / play with the interface -- solely within CALS.

While there is no direct connection to the CAMPUSWIDE system that Everette Allen is setting up, this system will likely go away once the production environment is up and stable.

Jason has agreed to give me access to poke around, so allowing this service account will have wider benefits in that I'll have a greater understanding of the configuration / settings / requirements of the CrashPlan and its LDAP integration by the time Everette comes a knocking for the service account that he'll need.

The Crashplan system will use the service account to confirm that users trying to use Crashplan are members of a specific AD security group (people who have licenses purchased for them). If not, they get denied access. If they are, creates them an account in the system.

Details of Crashplan's user management w/ LDAP integration can be found here:

http://support.code42.com/Administrator/3.6_And_4.0/Configuring/Integrating_With_LDAP_For_User_Authentication

ACTION: Committee Approved 8/11/14. As AD Tech committee had previously approved, implemented.

=====

Agenda:

Action Item: Dan needs to subscribe / invite Jeremy Brown to these meetings.

SCCM Service Teams Proposal [Debbie Carraway]
Could you add an agenda item for the August meeting for AD Policy to consider the SCCM support plan? The documents are in the AD Policy Committee folder. I'd like to ask the committee to make a recommendation to CITD that this support plan be adopted.

Change since last version: CITD wanted us to designate OIT as a service owner, responsible for providing the service coordinator. In order to address this, I added language describing the service owner's responsibilities (to provide resources to the service) and noted that the AD Policy committee would make a recommendation for who the service coordinator should be, but left the service decision-making as we had designed it, in the hands of the community.

Josh -- has questions regarding the possibility of funding for this effort?

Committee recommends that Debbie Carraway become the Service Coordinator.
Action Item: Dan will present this to the ITSAC-CAS. [did so at 10/2/14 meeting]

Reducing Software Package Install Default Timeouts [Daniel Henninger]
I wanted to talk a bit about a suggested change to the packaging policy for the NCSU level packages. Specifically, actually setting max run times to something "appropriate". (We try to set estimated time as well but meh) Lowering the max run times helps a lot when packages hang for some reason -- if they hang they sit there for 120 minutes before timing out. We tend to aim for more like the 20-40 time range to give them plenty of extra time without waiting -2 hours- before the next package can try to install.

Michael -- default can be changed across the board as well as per deployment type. There hasn't been a set timeout -- just the packagers have been using their best judgemment, but allowing perhaps more buffer than necessary.

We’d like to try dropping the default max from 2hrs to 1hr. In addition, the NCSU packagers should try to remember to change this default to the equivalent of no more than 3x the installation time of the particular package.

Changing the default would also AFFECT non-NCSU level packages -- aka, we’re mucking with department level packages at that point. Scripting this, however, would probably be a pain, so the committee decided to drop this change.

We’d like the packagers to focus on upcoming apps, not fixing existing ones unless specific requests are made.

SCCM Packaging Group Permissions [Dan Green]
Just wanted to note that Tom Farwig is working on generating a wishlist of permissions / access needed by members of the SCCM Packaging team that will allow them to handle all creation / promotion / retirement aspects of our NCSU level software catalog. There are still a few things (like SW group creations for example) that require someone like Billy or Dan to do and we’d like to get out of their way.

Dangers regarding SCCM Read Accounts? [Daniel Henninger]
Billy Beaudoin: “The CHASS-SCCM Viewers group is only of security concern for CHASS machines. That group right now has access to the CHASS collection and CHASS scoped objects with a Read-Only role. And as long as those accounts never are granted any permissions elsewhere, that works as expected. But if I add one of your .admin accounts to my -OU Admins group, that account now has an additional role that allows for deployment of objects that it has Scopes for. And it already has access to the CHASS collection. So through two group memberships it gets all the perms it needs to be able to deploy applications and images to CHASS machines. This is why no one outside of SCCM Service Team actually get rights on any NCSU-level collections.”

Daniel Henninger: “This I'd say is the core of why we might need to consider a policy on it. Kind of a ‘you can request one of these but be aware...‘“

Situation above arose from a project that Alan was working on. Goal was to explore and then bring back as a centralized option. But with him leaving, project died. Billy discovered the unintentional privilege elevation described above.

Michael is interested in a similar group within their OU. To create a similar group, the following process is used : Create AD group, Add a “user” in SCCM, grant the SCCM user access to the department OU collection and the Read-Only Analyst role.

An SCCM Admin would need to do this. There’s no reason why the SCCM admins would refuse to do this (no approval process needed) but we would request that a single security group at the department/college level so its not a burden on the SCCM admins to create. And the requesting group should be made aware of the issue described above and takes responsibility for someone in their OU doing something stupid.

It’s important that this information be recorded (hence this entry) should someone else find themselves in this situation.

Windows 8.0 and Windows 8.1 Baselines
Anything to report? No, we suck.

Windows 8.1 rollout
Still anemic. Some rolling out to labs, but seeing some driver issues relating to XP-era USB drivers breaking 8.1 USB. Faculty w/ tablet laptops that come with Windows 8.x installed.

We could start deleting drivers from the WDS driver group. Doesn’t require that the driver itself go away -- just removing from the group is enough. We don’t believe this would affect XP installs (plus we’re not supposed to be doing much of this anyway, so use a DVD if necessary) as WDS didn’t use the driver store for that OS. But we need to keep notes of what we remove. And if we have an initial batch of ones to remove, we need to post this to SysNews.

Security Comm revisting Drive Wiping / Encryption policies [Billy]
SSD drives -- when a sector goes bad, changes to read only. Means that we can’t wipe. Plus new DOD, etc, requirements all calling for encryption… So we need to start taking a more serious look at Bitlocker deployment for fixed disks on campus domained machines.

How to handle MS TS licenses? [Charles Cline]
Option 1 - provide a service where we provide a central TS license server that groups give us CALS and we set them up

- Who pays for the licenses?
- Who runs the service?
- Who’s currently running services: ENGR, OIT, AA, others? Citrix is a huge part. RDP Gateway also uses it for folks talking to XP.

Option 2 - set up a process to request a TS license server be set up. Apparently not really an option. Weird behavior ensues.

Committee Recommends that OIT write up the procedures (however they’d like to manage this) for new groups joining the domain to transfer their existing TS licenses to their existing central server. Docs for groups starting a terminal service and where to buy licenses should also be created. Both docs should be added to the ActiveDirectory site for OU Admins to refer to when needed.