AD Policy Working Group
Oct 17th, 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, Tim Smith, Debbie Carraway

Business handled outside of meetings:

Adding service accts to "NCSU-Read Group Memberships" [Dan Green, 10/6/14]
We have two requests for service accounts to be granted extra permissions.

The Library (Troy Hurteau and Emily Lynema) requests that their service account "lib.lookup.service" be granted membership in the security groups "NCSU-Read ncsuCampusID" and "NCSU-Read Group Memberships". This access will be used for their new card access system so it can be tied to AD groups.

They have another account, "lib.journey.service", which was previously granted this access to allow their KBox environment to function correctly.

OIT (Andrew Barnes) requests that their service account "oit.servicenow.service" be granted membership in the the security groups "NCSU-Read ncsuCampusID" and "NCSU-Read Group Memberships". This access will be used for the new ticketing system (Service Now) intended to replace Remedy.

As these are not controversial requests, I'd like to handle them over email. If you have questions, please don't hesitate to ask them. Otherwise, please respond with a yes or no.

ACTION: Committee Approved 10/8/14. Tech Comm approved 10/9/14, so have implemented 10/9/14.

=====

Agenda:

SCCM Update from M. Underwood
User State Migration -- has this been fixed? Isn't not clear if this is currently functioning as

expected. They'll investigate when they upgrade the server to Windows 2012 R2 next week. Part of the rolling SCCM upgrades to Windows 2012 R2 occuring.

Terminal Services ACL changes (Jonn Perry and Kevin Swann of OIT)
The Read Terminal Server License server and Write Terminal Server License server needs to be fixed at the wolftech domain level. The Terminal Server License group needs to have delegated rights on all user objects in wolftech. This issue is present in user objects that were present prior to Windows Server 2003 Domain Functional Level. Anything created since has received these permissions by default.

KB2030310 (http://support2.microsoft.com/kb/2030310) contains instructions to fix the issue of users being unable to get RDS CAL Licenses. The instructions are to reset the ACL for Terminal Server License Servers group.

This has already made the changes at the OIT level and it has been work without any issues. Users are successful getting CAL licenses. It was applied on the OIT OU in AD Users and Computers. It can be seen in properties/security tab. Go to advanced settings and you will see that Terminal Server License Servers has Read Terminal Server License server and Write Terminal Server License server set to Allow. It is applied to Descendant User objects.

Proposal: We would like to make the changes at the domain level. You'd want to do this at the NCSU and People OUs. This is a permissions delegation at these levels, not a group policy. Will be set for a single attribute, so extremely limited impact.

Committee: Approves. Passed to the Tech Comm to discuss and implement.

Office 365 and ADFS status (Charles)
We're in the process of rebuilding ADFS in Wolftest so the team (Derek, me, Kevin, Gene, and Joe) have understanding of the ADFS/Office 365 configuration. My main concern is we're being asked to have ADFS/Office 365 in production (Wolftech) in 3-4 weeks. Are we ok with that? Questions/comments?

Charles -- word seems to be getting around to faculty/students that this is out there.

(Dan) Who's asking for the short timeline? At the last ITSAC-CAS meeting, it almost sounded like they were just going to tell you to scrap the project.

Debbie -- so are we discussing ADFS or 365.
Charles -- focus is getting ADFS up and in production. As it will be used for other things. For 365, the next step would be to then get Azure AD up and then we would authorize who should have access to 365.

So key point -- we do have direct control over who gets Office 365 access in this model.

ADFS -- so this is a new federation service. Should be modeled on the Shib rollout (as far as attributes are permitted to be shared). We need to look at their request form. We'll need to confirm who on their end reviews the attributes requested (the non AD aspect of this) and then AD Policy/Tech for review of the general service.

ADFS timeline to implement -- Charles thinks about 3 weeks. Following its completion, work could begin on tying it to Azure.

ACTION (Charles):

- Need at minimum a page describing the overall service, outline these restrictions above and who to submit the request to.
- The Azure service is in scope and would need to be discussed. Would need to be discussed with the Security folks as it does involve the usage of attributes.

The Office 365 service would be out of the scope of this committee. But if the decision was made to move forward, the infrastructure would now be in place.

NCSU Now Licensed for Enterprise CALs (Debbie)

We are now licensed for the Enterprise CALs as well as the Core CALs (see below for details).

The Core CAL Suite includes:

- Windows Server CAL,
- Microsoft SharePoint Server Standard CAL,
- Microsoft Exchange Server Standard CAL,
- Microsoft System Center Configuration Manager Client Management License,
- System Center Endpoint Protection (antivirus client and subscription service)
- Microsoft Lync Server Standard CAL

The Enterprise CAL Suite includes:

- All of the components of the Core CAL Suite (listed above)
- Exchange Server Enterprise CAL with Services
- Exchange Online with Archiving for Exchange Server
- SharePoint Server Enterprise CAL
- Lync Server Enterprise CAL
- Windows Server Active Directory Rights Management Services CAL
- System Center Client Management Suite
    - System Center Operations Manager Client Management License
    - System Center Service Manager Client Management License
    - System Center Data Protection Manager Client Management License
    - System Center Orchestrator Client Management License

System Center Operations Manager Discussion (Charles)
We have SCOM up. We'd like to put a SCOM agent on a Wolftech DC so we can start getting reports - any questions, comments, issues, etc?

Why? Better monitoring of the DCs prior to the IAM implementation. Gene is interested in expanding this to cover other infrastructure -- WDS, SCCM, WSUS, etc…

Not looking to replace the Sysnews Nagios service. More internal monitoring and reactions to events.

Billy -- has concerns regarding putting the SCOM agent on the DCs as it would give SCOM managers control over the DCs. But potentially not the Domain Admins. However, the same concern exists with the SCCM client being installed on the DCs as well.

Who would have access: Charles and Kevin (original, just DC monitoring scope); expanded scope (SCCM admins, etc) would increase this but in that case, these folks might simply be using it as a service (scopes/roles?) rather than running it and having complete control.

Billy -- we need to better discuss and document just who has access to the DCs -- both directly and not indirectly through SCCM, SCOM, IAM, etc…

ACTION (Billy): Need to schedule a meeting to sit down and chat about direct/indirect control of the DCs and its documentation.

Email Address Attribute on Unity accounts in AD (Farwig)
We're working on testing and rolling out Google Cloud Print support for WolfPrint. PaperCut syncs account information for Unity accounts from WolfTech AD, including the "mail" attribute.

The issue we run into with CloudPrint is when the email address in WolfTech AD does not match what Google sends with the print job. The address coming from Google is unityid@ncsu.edu. Currently, the "mail" attribute in WolfTech AD matches what is in the campus directory, which could be an email alias, an off campus address, or some other NCSU address (unityid@eos.ncsu.edu for example) that does not match the Google address.

What we would like is to have an attribute in WolfTech AD that contains the unityid@ncsu.edu address, either a change in what is currently populated in the "mail" attribute or a new attribute that is part of the custom ncsuAccount class.

(Henninger) I would recommend going with a new attribute simply because people -might- be using that existing mail attribute and expecting it to match the preferred email address. Mind you we wouldn't be affected either way but I suspect some might. I'm also not sure where shibboleth

might get some of it's info.

Also, something that Everette and I noticed earlier today, WolfTech AD may be populating from what is in the campus directory when the account is created but it appears changes in the campus directory do not get pushed to the account in WolfTech AD. Everette's account would be one example, he currently has ega@ncsu.edu in the directory, but everette_allen@ncsu.edu in WolfTech AD.

(Gene Morse) The field is not being updated and is a known issue. It is being worked on. Jonn Perry can give more information on this if people are interested.

(Debbie) OIM will be pushing out the first, middle, last name of all account across the board, regardless of privacy blocks.

(Dan) Don't see a security / privacy issue w/ making all mail attribute as unity@ncsu.edu.

ACTION (Dan): Need to find and repair old script that was previously keeping this information updated for non-privacy blocked. Update so it affects all regardless, and start fixing the f/m/lname and mail attributes. Need to make sure what other attributes are being addressed in this script. Repair, have AD Tech review and approve, then go live.

SSL v3 flaw / Poodle Exploit (Derek)
Due to the recent POODLE Vulnerability (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566 https://www.openssl.org/~bodo/ssl-poodle.pdf), we should consider disabling SSL (all versions) on the WolfTech DCs, and perhaps all of the Windows machines joined to WolfTech AD. I'm most concerned with the DCs, as they provide ldaps auth services to a variety of services.

This article (http://support.microsoft.com/kb/245030/en-us), describes the Registry keys for the schannell.dll, and how to enable/disable various versions of SSL & TLS. I would consider disabling the SSL versions, and leave the TLS enabled.

Domain controller specific article:
https://social.technet.microsoft.com/Forums/windowsserver/en-US/1cf01f33-9cbe-4b76-b01c-83923c4cda04/is-it-possible-to-disable-sslv2-on-a-windows-2008-domain-controller-so-that-secure-ldap?forum=winserverDS

Concerns: Muck up LDAPs.wolftech load balancer? Windows itself should be fine, its the weird 3rd party stuff that might break. PHP/LDAP?

ACTIONS:

1. We don't think this should be pushed out to all clients across the board… but we should at least point out to the OU Admins why they might want to and the specific settings to

use if they want to do so.

2. We'd like you to turn it off on WolfTest VIP to confirm that the VIP service continues to keep working and responding as expected.
3. We want to it off on one of the production DCs -- one which isn't currently behind ldaps.wolftech.ad.ncsu.edu -- and have people point at to test. ECE would point some of our LDAP/PHP scripts at it, for example. This should only be a short window -- Monday through Wednesday. If folks are going to take the time to test, that should be enough. Most, we suspect will not, and will only voice their concern if a service fails after the change.

Presuming no reports, turn off on the DCs on Thursday morning. (presuming AD Tech concurs).

ACTION: Above decision has been communicated to AD Technical to review and implement.

Windows 8.0 and Windows 8.1 Baselines
Yes, we're still total slackers.

Requiring SANS Securing the Human Videos for OU Admins (Billy)
The SCGS has discussed trying to get a subset of these videos required for all staff, but it will be quite a while. Therefor they are looking for groups to opt-in to requiring them. There are around 50 3-10 minute videos, so clearly not all of them would need to be required, just a subset that the committee agrees upon.

https://moodle-projects.wolfware.ncsu.edu/course/view.php?id=789

ACTION: Everyone should go and complete this course before the next meeting so we can all know the experience before we require everyone else

What is the committee's opinion on whether computers that will fall under ISO/NIST compliance should be in WolfTech or a separate more secure AD (Billy/Daniel on behalf of Neal)

There is ongoing work for the PCI environment which will be a separate domain. Should all of these machines above be moved to this PCI domain, a 3rd domain, or should WolfTech AD be updated to support ISO/NIST compliance?

Committee all agrees that moving **large** amounts of research or administrative machines off of WolfTech AD would be very problematic and not desirable (as opposed to the small number that will move to the PCI domain).

ACTION: Goal should be to make sure that domain infrastructure be updated to pass ISO/NIST regulations along with the client portions of the domain as needed to comply.