AD Policy Working Group
February 19th, 2016
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, Daniel Sink

Ex Officio Members: Jeremy Brown, Michael Underwood, ~~Gene Morse~~, Rob Blanke

Guests: Billy Beaudoin, Debbie Carraway, Matt Pollard

Business handled outside of meetings:

Give access to read People / Group Memberships [Anthony Workman, 2/11/16]
Security & Compliance (Anthony) requests approval/permission from the AD Policy committee to add the read-only AD account -- wolftech\wt-euba.svc -- for use as described below, and place this service account in the "NCSU-Read Group Memberships", and/or other appropriate group(s) that has permissions to enumerate and read various user account properties throughout the WolfTech domain.

The reason why we need this account is because I'm testing a new product called Exabeam that does user behavioral analysis. The appliance is racked up and ready to go but there are some requirements I need to satisfy for it to be operational. This product appears to profile user account usage in order to spot anomalies in account behavior, indicating a possible security risk.

Fast forward to 0:59 for Exabeam demo.
https://www.youtube.com/watch?v=IAKgJWNF7Tw

Committee: Permission to add wolftech\wt-euba.svc to "NCSU-Read Group Memberships" approved on 2/17/16.

=====

Agenda:

Imaging team would like to remove NDJ images from the WDS servers [Jeremy Brown]

It was discussed and we don't believe we should be propagating non-domain joined OS installs. Is there a reason to provide, en masse, opportunities for non managed devices from a central campus service?

They're also going to move to 64bit as the default boot image. 32bit will still be an option, but wouldn't be a default.

Committee: Announce and Go Forth.

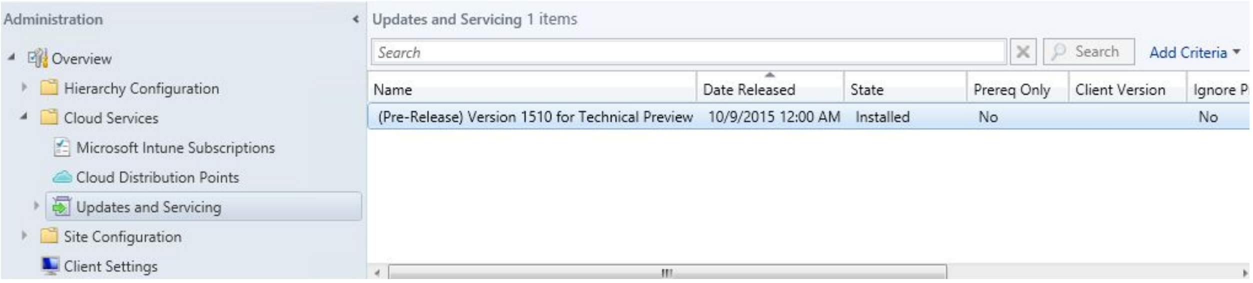
Discussion: Security Baselines in a Windows 10 world [Dan Green, Michael Underwood]

Need to look at how we review/approve/install security baselines for Windows 10 if we're looking at having to do so every 3 months instead of every 3 years…

SCCM upgrades too… see from Michael:

I'm hoping the upgrades are less intrusive in the future. Billy, is correct updates will come out sooner, but they will be smaller. So instead of an upgrade fixing 10 things it'll only fix or change 1 one thing. Upgrades are suppose to be cumulative.

It upgrading has turned into a cloud service. So the upgrade appears in the console and you simply right click and install:



Name	Date Released	State	Prereq Only	Client Version	Ignore P
(Pre-Release) Version 1510 for Technical Preview	10/9/2015 12:00 AM	Installed	No		No

More than likely there will be a client update with each new version. In 1511 there is now this new concept of pre-production and production rings for client updates. People volunteer to be in the pre-production ring, and they will have the most up-to-date client then after a time period Config Manager will upgrade the remaining clients.

Are these upgrades going to require an approval every time or do the committee just want to be informed? Let's not forget that the infrastructure changes are separate from the client changes. You can say, infrastructure upgrades are pre-approved but to upgrade clients you need approval. In the end, I would want to stay as up-to-date as much as possible.

There are better tools for diff'ing the baselines, so it should be easier to create reports of changes that the committee can read over.

DAN: We need to write up the policy, but we're going to keep it simple for now - when new draft or final comes out, we run a diff on whatever is presently installed. Report of the diffs goes out to the two committees to review. Should no red flags show up or objections raised, domadmins will announce upgrade via Sysnews/AD list and then install 3 or 4 business days later.

Clarification of Lastpass Use from Last Meeting [Dan Sink]
Daniel's homework from previous meeting:

Domadmin Accounts OK. .RE accounts OK -- both if used through DUO. And your LastPass master paswd must meet the requirements of PCI paswds.

No real other concerns for lower level accounts.
There have been some LastPass outages that might be of some concern.

Billy noted that PCI has reversible encryption requirements that LastPass might not meet. So Daniel has more homework to go check on this. However, beyond this, S&C encourages folks to start using LastPass. S&C also intends to have something more formal drafted up for review soon outlining appropriate use cases.

Discussion of Kumo Service [Charles Cline]
Cloud Service out of Indiana University that Charles wants to tie into that would allow us to use our unity accounts and a client on our computers (Windows and Mac) that would map cloud services to network drives. Google Drive, OneDrive, Box, etc. Files don't "sync" by default -- acts like network drive. Web conference next week w/ IA to discuss the technical details.

Once pilot is ready, will invite members of the AD comms to come and test before a broader test group.

Direct Access Update [Underwood]
Still in progress, no specifics yet.

OneDrive [Cline]
FYI, OneDrive is back to unlimited storage.

Updating Software Collection update times to 30 minutes [Michael Underwood]
Informal update from Michael regarding an improvement in our SCCM group change detection times. Will be moving from 2hrs to 30min updates. Why? Deltas have started working for some unknown reason after years of it not.

Committee Comment: Oh dear god, yes.

Give the NCSU packagers Read permissions on the NCSU collection [Michael Underwood]
When we first set the permissions for 2012 the permission list was not very granular. Now, there is an explicit Read and Deploy permissions. We can now give the Packagers read on the NCSU collection without giving them the ability to deploy.

Having read on the NCSU Collection will allow them to run reports on NCSU level deployments. If we want we can extend the read permission to all OU admins so they can run reports on NCSU level deployments to their users.

[daniel: does this affect being able to see deployments at all?]
[danG: there's some questions from Billy that popped up at the AD Tech meeting that's still be tested -- once reviewed, AD Tech will approve via email]

Committee: NCSU OU-Admins and NCSU Packagers get read on all NCSU level collections. Presuming Billy doesn't find a security issue -- he'll test, the Committee approves.

Discussion: Windows 7 & 8 Upgrade to Windows 10 via WSUS / SCCM [Dan Green / Michael Underwood]
http://blogs.technet.com/b/wsus/archive/2015/12/04/important-update-for-wsus-4-0-kb-3095113.aspx

It would appear that we have the option to inplace upgrade Window 7 or Windows 8 machines via WSUS / SCCM to Windows 10…

After some initial testing, it appears that Windows 10 patching through WSUS is receiving its patches without our needing to make any changes.

I'm just curious if there's any interest.
Negative reaction from the group. Zero interest in this even being an option.

Force OU Admins onto activedirectory@lists.ncsu.edu mailing list [Dan G.]

While technically we approved this over email, there were enough people wondering about how we'd enforce this, if we should require it, etc, that I thought we should take a few minutes to discuss in person prior to announcing. Iron out any details we need to.

Tom: "If we end up getting reported as spam enough times, then no one ends up getting the messages. Are we re-subscribing someone if they unsubscribe? Not sure if that violates any particular rules but it probably puts us at a higher risk to being tagged as spam. Opt-out was mentioned in the discussion, is there a way to implement that? Would we instead disable someone's .admin account if they unsubscribe? Also, we would need to make sure we don't end up double subscribing someone if they use a different address from what we are able to determine based on their .admin account."

Dan H: "Well (and again I'm for actually going through with this), if you -do- force someone into a list they don't want to be on, and they end up filtering the entire thing into oblivion, you haven't accomplished a lot. Plus if they choose to label it is spam, google may start considering it to be spam globally. (as we've seen with some of our internal newsletters) I'm not entirely convinced just subscribing them to a list implies a responsibility. =) but I am totally playing devil's advocate here for the sake of "thinking about it" first. (think and do! ... i'm sorry) I find it unlikely an OU admin would truly object to being on the ad list." addendum: Do eet.

Debbie: "Maybe I'm too unsympathetic, but in my mind that's what filters are for. They can automatically delete everything, but with an automatic subscription they are responsible for knowing the info. It honestly doesn't take much time to scan through the ad list (or any of the others)."

Committee: Yes, you must be on the list. Dan will go forth and script this.

Stuff on the horizon… (things not quite ready to be discussed)

- **DirectAccess Demonstration [M. Underwood]**
- **Security Standard for Sensitive Data and Systems [~~Jessie Henninger~~]** https://docs.google.com/document/d/1ZdLqnHmXZLKeYsPWXwM8l4XIn3fWmuf3nLQcE-0vYyk/edit#heading=h.ik9joinausi **Rescheduling for 2016 as Jessie left S&C.**