AD Policy Working Group
June 19, 2015
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, Derek Ballard, Anthony Workman, William Ogle

---

Business handled outside of meetings:

Give oit.freeipa.svc access to read People / Group Memberships [Derek Ballard, 4/30/15]
The OIT CSI (Central Services & Integration) group request a service account (oit.freeipa.svc) be granted read access on the user accounts in the People OU, and the ability to also read group memberships to test FreeIPA (a single sign on/centralization of Linux Realm users) functionality; to see if they can use AD groups for various colleges and departments on campus to control access to the next generation of Realm Linux systems such as Puppet and Foreman.

ACTION: Committee Approved on 5/4/15.

NCSU-Read Group Membership group: PCI SCCM environment [M. Underwood, 5/7/15]
Request from Michael Underwood for the SCCM team:

"We are in the process of building the PCI SCCM environment. We need to have the reporting point, OIT212SCCM-RP, added to the NCSU read group. We've already done this for the current SCCM instance."

This is needed so the reporting will function correctly. As we've already approved this for the main SCCM setup, it's mostly rubber stamping for the PCI equivalent. Any questions?

ACTION: Committee Approved on 5/8/15.

Request to add AGPM.admx and AGPM.adml to the central store [Kevin Swann, 5/12/15]
I need to add AGPM.admx and AGPM.adml to the central store. Any issues with this? These admx extensions are needed so that I can make settings changes to the Advanced Group Policy Management environment. Specifically, setting the default AGPM server. This is so when we use the AGPM, folks will not have to configure it each time they install the snap-in.

ACTION: Committee Approved on 5/13/15.

=====

Agenda:

Remove automatic site assignment from the NCSU site (SCCM) [M. Underwood]
We currently have automatic site assignment turned on for the NCSU level SCCM environment. When you have this turned on the site boundaries are published to AD. When someone tries to install the SCCM agent by double clicking on the exe, the installer queries AD to find out what site it is in.

If you have well defined sites boundaries this isn't an issue. Since PCI decided not to create subnets or vlans just for PCI connected systems we have connected systems in the same subnet/vlan as non PCI machines. The SCCM sites servers for instance.

This could cause machines to end up in the wrong site. PCI in the NCSU site and vice versa. We are specifying the site code in the install script, so automatic site assignments are not needed. We want to remove automatic site assignment from the NCSU site.

Committee: **Approved**; SCCM Admins asked to implement.

Extending Inventory in SCCM to include OS SKU [M. Underwood]
We talked in the Technical Committee meeting about extending the inventory in SCCM to include the OS sku. The MBAM agent can only run on Enterprise and Ultimate versions which isn't a part of the standard inventory so it needs to be extend so we can capture that information in order to make the deployment of the MBAM agent more targeted.

Committee: **Approved**; SCCM Admins asked to implement.

Patches for WSUS Early groups [D. Green]
FYI: Due to some confusion in the language of our written policies, patches that Microsoft releases outside of Patch Tuesday have not been released to the Early groups immediately for testing. This was the process for many years, but has not been for quite some time now. We're working to fix/clarify the language on the website, and a new rule has been added to the WSUS server to automate this. Patches from the SCCM server have been releasing as expected (it already had automation in place for this).

MBAM Demonstration [M. Underwood]
Great demonstration, but some questions/considerations were raised that need answers:
- what happens to list of valid users associated with a machine after it's reinstalled
- do members of said list of users get auto-pruned after some time
- perhaps add some wording somewhere saying don't help someone unlock their computer not in your organization even if it's just to do a favor
- should the ncsu helpdesk be expected to handle users calling to get their computer unlocked, or should they insta-hand off the call to the appropriate department -- if the ncsu helpdesk, tier 2?

Followup (6/22/15) from Dan Evans: “I just spoke with Chris King regarding the OIT Help Desk being front line support for MBAM requests. He's willing to entertain handling the unlock requests given enough information, training and the access to do it.

Since the HD isn't 24x7, you still may need a departmental an on-call list for your group's users calling from foreign lands at 3 AM.”

Dan’s comments (6/22/15) -- as long as we include links to the enduser SelfService portal (not the helpdesk portal that OU Admins or the OIT HelpDesk would use) when educating our users, then anyone who’s already associated with their own machine won’t need to interact with us. Hopefully that resolves most 3am issues that arise.

DirectAccess Demonstration [M. Underwood]
[Punted to Next Meeting due to lack of time]

Active Directory Service Owner Message [M. Hoit]
“As most of you know, Internal Audit conducted a review of the WolfTech Active Directory service in 2013. There were concerns about the lack of an identified service owner for this campus service. The service owner is the organization that is responsible for ensuring that the service has the resources it needs. This includes funding hardware, licensing, maintenance and technical support as well as ensuring adequate staffing is available to support the service. The service owner is responsible for providing a service coordinator. The service owner has final responsibility for ensuring that the service meets the needs and expectations of the campus.

During 2014 we had several discussions about identifying a service owner for the Active Directory service for campus. I want to officially communicate the decision to the appropriate IT Governance Committees and Working Groups to ensure all involved are aware of the final decision.

OIT is the service owner of the Active Directory service for NC State University in collaboration with the College of Engineering and the governance working groups (AD Policy and AD Technical) in the design and support of the service. Specifically, I have charged Debbie

Carraway, Assistant Director of Systems & Hosted Services (SHS) in OIT Infrastructure, Systems & Operations as the service coordinator for the campus Active Directory service.

As service coordinator, Debbie is responsible for ensuring that the overall service is operating smoothly. Debbie acts as a point of contact for the service, and can direct inquiries to the appropriate service teams. Debbie ensures that governance groups are meeting as needed, and that the groups are coordinating with each other as needed. Debbie works with the service team leads to ensure that submitted issues (via our call tracking system) are handled appropriately. Debbie will ensure that decisions about the service are made by the appropriate governance body.

I appreciate the commitment by all involved, especially the members of the AD Policy & Technical Committees, with making the Active Directory service an example of successful collaboration in the delivery of an important campus service."

Further details provided by Debbie:

To: AD Policy and AD Tech

Date: June 12, 2015

Re: Practical impact of service ownership

I would like to clarify the practical impact of OIT being named "service owner" for AD and my role as "service coordinator."

OIT as "service owner" has these responsibilities:

Ensuring that the service has the resources it needs. This means that we are responsible for making sure that servers and storage are available as needed for AD, SCCM, and any critical services. We are also responsible for making sure that we have the necessary licenses. We're responsible for "maintenance," which practically speaking means that we pay for the Microsoft Premier agreement at a level sufficient to ensure that the service is healthy, and which includes the various health checks that we've done annually.

We are also responsible for making sure that we have an adequate number of trained staff available to maintain the service. This does not mean that OIT is the only group that can be domain administrator. It does mean that we are responsible for making sure that we are staffed sufficiently to handle domain and critical system administration as needed. We fully expect to continue working in partnership with other campus IT staff to provide and support these services, such as with the SCCM service teams.

This also means that we have operational responsibilities. We are responsible for making sure the services are monitored 24x7 through an on-call rotation, as we currently do. We contribute to making sure things are working – and we should do this through our existing processes that include partnerships with other campus IT staff. But, ultimately it means that if, for example, the domain controllers go down, if AD or SCCM has data corruption, etc., we are responsible for making sure it gets fixed.

Final responsibility for ensuring that the service meets the needs and expectations of campus. This means that whatever we do has to meet campus needs and expectations, not just OIT needs. The way we accomplish this is normally through governance, through the AD Policy and AD Tech groups. If we want to make substantial changes, we would (like anyone else) propose them through governance.

<u>As service coordinator, I have these responsibilities, and plan the following:</u>

Ensure that support requests are handled. This means that I will make sure that the relevant ServiceNow groups monitor and respond to requests in a reasonable timeframe. Practically, I want to establish some documented expectations for response time and follow-up for the relevant workgroups.

Ensure the overall service is operating smoothly ("Operational Excellence"). I am responsible for ensuring that the services use best practices and that we meet IT Audit requirements and respond to findings. This means that I will coordinate finding resources and ensuring that we respond to the items required/recommended as a result of the AD audit, including documenting a service level statement and implementing some (light) formal change management processes. Also, as part of the audit I will be making sure that we complete the AD strategy document, which will be shared with the governance groups. This also includes making sure there are processes for responding to support needs.

Act as a point of contact for the service. Practically, this means that people can contact me and that I will steer them in the appropriate direction. For example, if OIT management wants a change, I can help them through the governance process. Or, if there is a crisis, I will act as a point of contact to ensure that adequate communication occurs. I'll represent the services to the OIT Change Advisory Board, which is a group that meets weekly to communicate about changes to campus services that might have a broad impact. It's a coordinating role. I don't see a big difference in my role; it may mean that we need some slightly more formal communication processes.

Make sure governance groups are meeting and coordinating with each other as needed. This is not a real area of concern, as the governance groups are doing just fine. It does mean that I need to make sure some administrivia is handled, like making sure meeting minutes are posted and that meeting schedules are publicly available. If there were concerns about the governance groups, I would work with the chairs and members to address them.

Ensure that decisions about the service are made by the appropriate governance body. I am responsible for making sure that change requests go through governance. Part of this may be a documentation function, to ensure that the campus community clearly understands what kinds of decisions are made by IT governance, who their representatives are, and how to make requests and suggestions.

Make sure that regulatory requirements are met and security best practices are followed. There may be some changes that will be required to ensure that regulatory requirements are met. I need to make sure that we have a design and structure that allows the campus to meet these requirements, such as PCI, NIST and ISO standards. I'm also responsible for ensuring that the service is appropriately secured (such as following the “principle of least privilege”). Part of this is an operational responsibility that the domain admins or service admins would implement. Any major changes to the functionality or management of the service would go through governance, as usual.

Accountability. Ultimately, for me, it means that I have responsibility for making sure that the AD service works well. I will be held accountable by my management for ensuring that it does.

Overall, the practical changes I see are that OIT has acknowledged full responsibility for making sure that the service is resourced appropriately and meets the needs of the campus community, and I am tasked to make sure that we have good processes that are documented appropriately. The existing decision-making processes are the responsibility of governance and the collaboration we all share should continue.

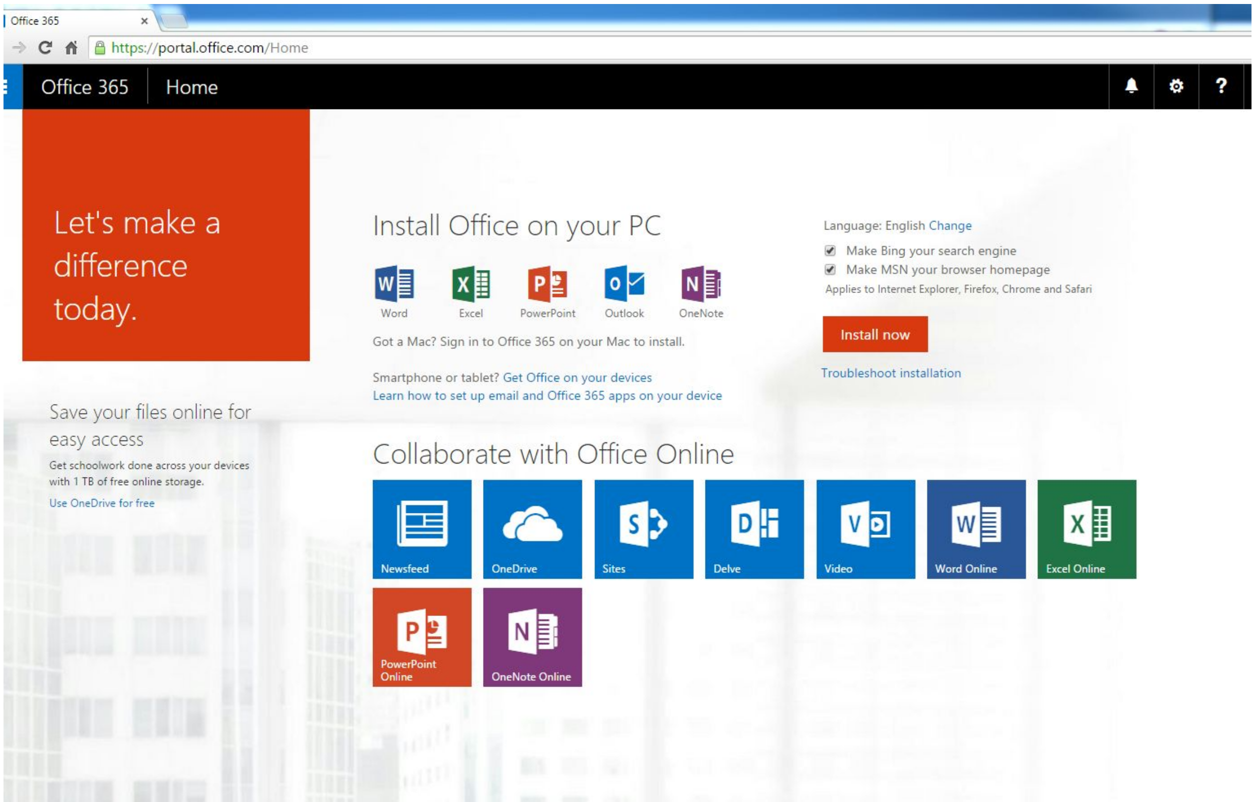
Please feel free to contact me with any questions, comments or suggestions.

Debbie

Office 365 Update [C. Cline]

179,000 accounts in AzureAD synchronized daily that are now licensed. MS process didn’t license to everything sync’d. Fixed now. Anyone with unity ID can now log in and use, but this isn’t quite production yet.

1) Visit http://portal.office.com
2) Enter unity@ncsu.edu email address - it will prompt you for your local NCSU account credentials.
3) Enter unity ID specified as wolftech\unityID and password
4) Ta da!
5) Still some work to be done about data sensitivity and storage of data.



Let's make a difference today.

Save your files online for easy access

Get schoolwork done across your devices with 1 TB of free online storage.

Use OneDrive for free

Install Office on your PC

Got a Mac? Sign in to Office 365 on your Mac to install.

Smartphone or tablet? Get Office on your devices

Learn how to set up email and Office 365 apps on your device

Language: English Change

☑ Make Bing your search engine

☑ Make MSN your browser homepage

Applies to Internet Explorer, Firefox, Chrome and Safari

Troubleshoot installation

Collaborate with Office Online