WNAG

Meeting: 2016-12-21
Present: Jim Johnston (Chair), Nevil Bromley, Manfred Griesbach, Anton Romantsov (Secretary), Lowell Williamson, Steve Nickerson, Ravindri Kulatunga, Mike Patterson, Jason Testart, Mike Gaspic, Connie van Oostveen, Andrew Ward, Sean Mason, Dave Hinton

New Business

Mike Gaspic: IAMNG project presentation and overview (the details in IAMNG Core Project Charter Final and IAMNG-Nexus_Provisioning_Issues documents included with the Agenda for this meeting).

Project phases:

Phase 1-3 – new solution in works, Phase 4 – cut over, new solution replaces existing WatIAM
P1 – initial data brought in
P2 (current) – HR and Quest data in, next to come data from telephone services, O365, Connect
P3 – addition of new sources (Retail Services, Watcard, Library, Lync)
P4 (end of October 2017) – go live as WatIAM 2.0

Subsequent discussion and feedback:

Sean: Challenge representing individuals with multiple identities, multiple affiliation across campus.
Jim: Use security groups instead of OUs?
Dave: With groups we can't have hidden users, works only with OUs (following Microsoft recommended method – removing list permission on OU level).
Jason: Why we need hidden users?
Dave: Helps to prevent information from being accessed via ldap queries (user's name, email, description and other info about the user stored in AD).
Jason: Revisit the whole idea hiding the users? Currently users can opt out in whitepages if they wish to be hidden. Can we not publish any info unless the user wants to out in?
Jason: Restrict access to ldap queries?
Dave: Cannot be easily done, however only basic info is available through ldap.
Jason: Stop publish home phones in whitepages.
Dave: Some information is leaking to Office 365 environment, people started removing data from WatIAM.

Jason: Use security groups to control access to a resource, use Grouper to provision a group of users who will be given access to the resource, e.g. based on classes list info.
Dave: It will be possible to find out members of that group using ldap anyway.
Jim: Math already using similar approach to manage printer access… If a user in a hidden OU, does this make effect on all programs or only on ldap queries?
Manfred: It depends on the app, there is a process that can find all users even in hidden OUs.
Jim: Can all users information be hidden?
Manfred: By design information in AD is open unless something was explicitly closed (hidden).

Jason: Using Grouper can help minimize need to accessing info through Nexus (for most things). Proposing set up a time to demo Grouper to wnag and let people come up with ideas how we can make use of it.

Multiple Affiliations/Home Directory:

Manfred: Defining primary role has always been a challenge. The role needs to be defined for home drive assignment.
Sean: Let WatIAM to decide on primary role?
Jason: Allow manual choice of affiliation so that users can choose what their primary role is and the identity system records this.
Jim: If we have to have primary role, we should first define what primary role is.
Jason: Can we assign a unique drive letter to each resource?
Dave: Still have to assign a letter to your "home" drive.
Manfred: Like the idea of specific drive letters. The home drive can be any letter.
Dave: That won't work well from applications perspective – some apps will be trying to map a network resource by drive letter (not by UNC path).

Account Renames/Implied Access:

Dave: O365 creates new uids based on samaccount name hash.
Jason: Use email address instead of uids?
Dave: Account renames in O365 will be an issue going forward.
Mike G.: How are we cleaning up orphaned userids? We should create a process to do that. Get an "Applicant OU" where userids that are not used can be held for some time and then be deleted?
Dave: Looking into this idea may significantly delay Grouper implementation.
Jason: This is just to open initial discussion on this, not thinking about implementation yet.
Mike G.: We will allow test access to Grouper, anyone wanted access talk to Sean.

Other Business

UE-V & roaming profiles:

Nevil: Folder redirection – we need to get everybody on the same page. Environment, AHS, Arts can all work together and agree on common approach.
Jim: Math is interested to join too.
Lowell: Can we pick whatever is being done today as a base and implement? Agree to do it in AHS.
Manfred: There are about 600 users who come to IST who may be impacted (profile issues, home directory drive letter).

Upgrade to Win10 build 1607:

Nevil: Issues with software packages deployed with SCCM - some are sitting and waiting in Software Center, older version deployed over newer one.
Lowell: We are using our own WSUS server.
Manfred: Why not use SCCM?

Lowell: Like the granularity, and local WSUS works faster overall.
Manfred: Microsoft keep changing things around how patching works, rollups and upgrades, packaging updates together become more common thing.

Audit of additional events on Nexus DCs:

Anton: Enable additional auditing of Kerberos authentication events to enhance monitoring, including audit of O365 logons. This will only apply for DCs, has no effect on users, workstations or services. Might slightly increase utilization of resources on DCs (e.g. space for logs).
Jim: No objections as long as no effect on users.

Other:

Dave's update on Office 365: Considering multiple tenants in the cloud - edu.uwaterloo.ca for students only, move stuff and faculty accounts away from onmicrosoft.uwaterloo.ca into a separate tenant, which could be uwaterloo.ca. Same tenant for all provides no separation for student and stuff email (e.g. when a user is a student and a stuff at the same time, or when a legal event occurs). Currently Microsoft offers no native tools which could facilitate moves of accounts between tenants (e.g. from onmicrosoft.uwaterloo.ca to edu.uwaterloo.ca). This creates potential problem with user migrations from tenant to tenant.

Dave was asked to write more information to the group on the O365 multi-tenant matter and the challenges that were discovered so far.