AD Policy Working Group
April 27th, 2012
3110 Engineering Building II
3pm-4:30pm

Present: Donna Barrett, Billy Beaudoin, Tom Farwig, Dan Green, Julie Tilley
Absent: Daniel Henninger, Joshua Gira, Dan Evans

Guests: Alan Gerber (sub for CHASS), Joe Johnson, Fred Eaker, Michael Underwood

Business handled outside of meetings:

- Workstation Health Check Related: See Appendix A
- IE Settings Updated (due to changes in Portal from Financials update): See Appendix B

=====

Agenda:

Remote Desktop Gateways / Network Policy Server (Alan)

- Response to the campus gateway block -- specifically vendor issues + users whom do not have a UnityID (and therefore cannot use the NCSU VPN solution). MS has an alternative -- a proxy for remote desktop. Uses port 443 (which we don't have blocked).
- Alan has already been testing in WolfTest domain.
- Solution could be used for non-domained computers (though you will need a domain account to login to the proxy).
- Requires TS CALs -- even for boxes that normally don't -- for RDP proxy to the OS
    - CHASS potentially looking to buy some licenses.
    - Hosted systems has a lot of Vendors that Joe needs to have using this service.
    - License per client required. $25/CAL?
- Add RDS-G server to RAS and IAS Servers Group (precreated AD group) - Subset of permissions compared to what NCSU-Read Group Memberships. Network Policy Server needed if there are multiple RDS-G (issue for later).
- Possible new AD service like WSUS/WDS/SCCM?
    - Management? Who? Joe and Alan have agreed to be the initial service owners.
- Get the service up and working, then look at how best to deal with licensing?
- **Approval: Get the server setup and available, then start working to define the RDS-G service (website, list service owners, and define the licensing process).**
- **ACTION**: **Alan/Joe coordinate w/ Derek to get the new server into the appropriate OU / security group. Once service is up, document on AD website.**

Workstation Health Check followup (Billy)
- Still looking at additional settings for improvements.
- Report was posted on the AD website
- We held a training class to show colleges how to utilize the WDRAP to test their

systems. Recording online.

"Guess what, we've been renamed": NCSU IT Governance update (Dan)
- We're now a "working group" under the ITSAC-CAS (Client and Applications Support)
- Minutes will be made available to this subcommittee for comment/questions.
- Topics we feel should be discussed outside of our working group or will need additional support to be enacted will be passed up the chain.

Shadow groups for OS's to defer WMI query times
- Came up during Health Check.
- Way to improve boot process speeds -- looking at domain level policies.
- Estimate of a few seconds per policy save. Times a dozen+ policies. 30 sec improvement?
- Issues with newly joined computers? Before the object has been added to a shadow group, wouldn't get the correct domain level policies. How about reinstalling/upgrading to a newer OS?
- CHASS already planning to do -- as a part of their prestage process, they will capture OS and add to their shadow groups.
- We already have a security group that we're adding all Macs to. Need to confirm how often that script to populate is running. (updated: it runs every 10 minutes beginning on the hour.)
- **ACTION: People intrigued and agree that shaving 30secs is a good thing -- Billy, go figure out details.**

Warranty Extensions on DCs (Billy/Debbie)
- 3 of current DCs bought by ENGR. Billy extending warranties another 2yrs ($3366).
- OIT will buy new server (that will be the new SCCM 2012 site server; more below). Once upgrade complete, old site server will replace one of the 3 DCs.
- Next fiscal year, OIT will purchase a replacement for another DC.
- GOAL: get to a replacement cycle (one DC a year-ish) for the DCs (funded by OIT)

LDRPS Test System (Dan)
- Both Billy and Dan have been contacted by the folks testing the new LDPRS system (used to manage disaster recovery plans by business units) to request that their test system URL be added to the domain wide policy of IE trusted sites. As this is not a production service, and is only needed for a couple dozen testers, this was rejected.
- Instructions were provided as to how the local IT for those testing could set this policy at a local level rather than us doing so centrally (and affecting 14,000 computers).
- Once testing is completed and a production service URL is finalized, we will revisit.

WolfTest Rebuild
- WolfTest is dead. Long live WolfTest.
- Most everything is back, after a few scripting issues. For example, one iteration caused all the user accounts to be created over and over. As this is our first attempt at deleting and reprovisioning the test domain automatically via scripts, a few bugs were to be expected. At the time of the meeting, only a few last steps remained in the provisioning.
- If you need to use it for testing of a new service, talk to Joe Wells, Derek Ballard, Todd Kerstetter or Jonn Perry.

EHPS wants to send notifications to client machines - ala Text messaging
- "WolfAlerts to the desktop"
- **ACTION (Dan): Need to get some details from the WolfAlerts folk to get details. (update: contacted Todd Becker for details)**
- There are ways of using Windows Messanger service or other notifications? Still there in Windows 7? Windows 8? Nope, dropped in Vista.
- Build mini app to look at the WolfAlert RSS feed?

SCCM 2012
- "to me its pretty awesome" [Mike]
- Not an upgrade -- we need to migrate from current system to the new one.
- It can copy existing setup, then delta changes every 4hrs (extended migration)
- 2012 is read-only until we sever ties with 2007.
- What we still need to move forward: new site server, which (above) has been purchased.
- Need to have MS come setup MS Reporting Services this time.
- 2007 clients talk to 2007 + 2012
- **ACTION (Mike): update client install script to hardcode NCS site, so 2007 clients don't accidentally connect to new 2012.**
- So, what's fixed, better, "awesome"?
  - lots of site level settings can be set at collections now.
  - permissions we've hacked together is less necessary. There's scopes and roles/permissions in the new version.
  - new software installation model -- better ways to confirm if software actually installed. Uninstall function? "Software Center" -- new interface for endusers.
  - SCCM console gone -- real application.
  - Discovery of objects -- delta updates should now get group info -- so you add to a group, it sees in 15mins rather than current hour or two.
  - Auto approval of software updates.
    - will help w/ Early group patches
    - will allow immediate deployment of definitions.
- Timeline: need to recreate 2007 SCCM infrastructure in WolfTest, so they can then install 2012 to test the migration. This will take a while (Billy threw out October timeframe as guestimate). And there may be advantages to running SCCM 2012 on Server 2012... which may necessitate another reinstallation later.
  - This time around, its important that we get a commitment for another body to be assigned (besides Michael) during the initial (say, xx days per week) of the project build time.

For next agenda:
- 6th DC for testing of the VM Snapshot/Offsite service (Billy)

Appendix A: Workstation Health Check Updates

https://sysnews.ncsu.edu/news/4f64f4c9

1. XP Machines need to have a periodic Defrag running. We'd like to copy the Scheduled Task from the CHASS policy "CHASS-Defragment Disk Biweekly (WinXP)" to implement as a weekly defrag (weekly to keep in line with what Win7 does).

2. We'd like to disable "Distributed Link Tracking Client" Service across the board. It is not used and cannot function without the DC's being set to do it, which they aren't.

3. We'd like to set the "SNMP Traps" service set to Disabled on client OS's. It is currently set to run on a large number of machines. But its really only used on Servers on campus.

4. We'd like to set CacheQuotaLimit = 10% This is the max cache value for Offline files. By default its 25% of the client disk size, which considering the size of newer disks, we're talking about possibly hundreds of GB.

5. We'd like to remove the "Remove Default Users" script from the Windows Vista/7/8 GPO's. There is a separate "Remove Default Users" GPO for "Client OS's". So its running twice on these 3 OS's.

6. Pull the WolfTech-CWDIllegalInDllSearch (KB2264107) Policy as the patch is in WSUS.

Appendix B:

IE Settings Updated (due to changes in the Portal from Financials update):

Option 1: Create a new policy for IE zone settings and filter it with the "Windows Desktop OS" WMI filter.

Option 2: Co-opt the "WolfTech-Remove Default Users" policy (which uses the Desktop OS WMI filter), add the IE settings, and name it something like "WolfTech-Default Domain Policy - Desktop OS" so that we don't have another policy.

Option 3: Suck it up and add the list to each of the Win{XP, Vista, 7, 8} policies.

I have a couple of different requests from EAS staff regarding portal servers and the intranet zone list.

This first list came from Wade Davis when OIT Business Services was having issues with access to certain items in the portal.

https://www3.acs.ncsu.edu
https://ffrpt.acs.ncsu.edu
https://hcrpt.acs.ncsu.edu/

The two servers below came from Ron Reed and are part of the new financials system:

https://fo91prd.acs.ncsu.edu
https://fo91rpt.acs.ncsu.edu

This list came from Craig DeShong when Wade asked his group whether or not they could think of any other servers that might need to be added. Not sure whether or not that means we should automatically add all of them or not:

https://ssdv.acs.ncsu.edu   singularity suite development
https://ssqa.acs.ncsu.edu   singularity suite aq
https://idm-dev.acs.ncsu.edu   sar development
https://idm-qa.acs.ncsu.edu   sar qa
https://idmprod.acs.ncsu.edu   sar produciton
https://idm-trn.acs.ncsu.edu   sat training
https://sbdv.acs.ncsu.edu   sas development
https;//sbdv2.acs.ncsu.edu   sas development
https://dbprd.acs.ncsu.edu   sas production
https://sbrs.acs.ncsu.edu   sas
https://www6dev.acs.ncsu.edu   development java applications
https://www6qa.acs.ncsu.edu   qa java applications
https://www9.acs.ncsu.edu   production java applications