

Agenda/Minutes 6/18/10

Friday, June 18, 2010

Attending: Tom Farwig, Dan Green, Josh Gira, Billy Beaudoin, Dan Henninger, Dan Evans
Guests: None.

1. Brief Update from Technical Comm [Billy B]
 - New defaults
 - Signed Scripts -- plan is to currently use one cert made available. Can use your own, but may take a while to have it generated, so one will be made available. Plan is to have docs at some point.
 - Computers Ping by default. Was applied to all firewall modes (private/public/domain/etc). Not being able to be pinged isn't a security benefit. But not being able to ping can make it a pain for admins or even endusers to diagnose network issues.
 - Disabled AutoRegister this computer with the network. Was actually already turned on elsewhere, so no changes.
 - Unassigned OU -- question: will we assign the campus default security policies here? Answer: already done.
 - Account Provisioning moved to OIT scripts
 - Were some initial problems, fixed.
 - Account resets now working.
 - Workshop Accounts **should** be working.
 - Fname, Lname, Email info in accounts still being run by Stein's scripts.
 - Problems noticed with accounts being disabled/enabled based on krb_disable.
 - Win2008 R2 Web Management turned on; still being configured. Needed for new powershell management scripts.
 - Derek researching security before announcing.
 - Talking to UNC re: ADFS to tie NCSU / UNC
 - BME sharepoint
 - UNC has interest in NCSU ERP folks accessing UNC's sharepoint.
2. SLA Task Force Update [Josh]
 - a. Has met! June 9th
 - b. Rough draft based on other EDU SLAs
 - c. Looked at AD services; thinking 3 tiers. (Help Desk / OU admins / Domain admins)
 - i. Desktop Management and Account Prv are diff SLAs
 - ii. Defining "what are expectations of those working on these services"
 - iii. Job skills, training needed
 - iv. Measuring costs -- cost of running vs charges for service.
 - d. Objective -- SLA must be under 3 pages.
3. Software Task Force Report [Tom Farwig]
 - a. Two documents provided: WolfTech AD Software Life Cycle + WolfTech AD Software Naming Conventions (appended below to minutes)
 - b. Committee discussed and provided feedback which will need to be integrated into the documents.
4. *"INTERACTIVE": Account security / who can login where. Details on the existing loophole. [Dan G] -- punted to next meeting*

WolfTech AD Software Naming Conventions

(Proposed 6/18/2010)

Software Group Names: [OU]-[SWCode]-[Vendor]-[AppName]-[AppVersion]-(GPOVersion)

SWCode is one of the following:

- EX - Experimental Software. This software is in the initial creation stages or the testing stage.
- SW - Licensed Software. This software is in production. An appropriate license to use the software is required.
- FW - Freeware. This software is in production. This software is licensed as freeware by the software vendor.
- DN - Deny group. Used to deny access to a production software package. A group that is in an SW or FW group and also in the DN group for the same software will not receive that software.

AppVersion should use as much of the vendor given application version as possible to keep the group name as unique as possible.

GPOVersion is optional, but is required when naming conflicts arise. To keep group names within the 64 character limit, it will be displayed as a "v" with a number after it. IE -v1, -v2. This applies to new software packages only, older packages do not have to be renamed if they have the date stamp on them as the version.

Group Policy Names: [SoftwareGroupName]-(WMI filter description)

In cases where multiple installers exist for the same package, for example, a 32-bit and a 64-bit installer, a single software group should be used with multiple GPOs making use of WMI filters to determine which one gets installed. To avoid naming conflicts, a short WMI description should be added to the end of the SoftwareGroupName to distinguish between the different GPOs.

Folder Names: [Vendor]-[AppName]-[AppVersion]-(GPOVersion)

Folder/DFS link names should match the software group name except without the OU and SWCode. If necessary the software packager will create subfolders for different installers (ie: x86, x64).

Hidden Share Path will be: \\[SERVER]\[FolderName]\$

DFS Path will be: \\wolftech.ad.ncsu.edu\software\[FolderName]

The following examples assume that everything is deployed at the NCSU level. Server names listed for the hidden share are examples only.

Application: Mozilla Firefox 3.6.3

License: Freeware

Installers: Single installer for all platforms.

Group Names:

- NCSU-EX-Mozilla-Firefox-3.6.3 (Creation/Testing)
- NCSU-FW-Mozilla-Firefox-3.6.3 (Production)
- NCSU-DN-Mozilla-Firefox-3.6.3 (Deny Group/Production)

GPO Names:

- NCSU-EX-Mozilla-Firefox-3.6.3 (Creation/Testing)
- NCSU-FW-Mozilla-Firefox-3.6.3 (Production)

Folder Name: Mozilla-Firefox-3.6.3

Paths:

- \\wolftech.ad.ncsu.edu\software\Mozilla-Firefox-3.6.3 (DFS)
- \\software1.ncsu.edu\Mozilla-Firefox-3.6.3\$ (Hidden Share)

Application: Microsoft Office 2010 (all features installed)

License: Purchased Software

Installers: 32-bit and 64-bit

Group Names:

- NCSU-EX-Microsoft-Office-2010 (Creation/Testing)
- NCSU-SW-Microsoft-Office-2010 (Production)
- NCSU-DN-Microsoft-Office-2010 (Deny Group/Production)

GPO Names:

- NCSU-EX-Microsoft-Office-2010-x86 (Creation/Testing 32-bit)
- NCSU-EX-Microsoft-Office-2010-x64 (Creation/Testing 64-bit)
- NCSU-SW-Microsoft-Office-2010-x86 (Production 32-bit)
- NCSU-SW-Microsoft-Office-2010-x64 (Production 64-bit)

Folder Name: Microsoft-Office-2010

Paths:

- \\wolftech.ad.ncsu.edu\software\Microsoft-Office-2010 (DFS)
- \\software2.ncsu.edu\Microsoft-Office-2010\$ (Hidden Share)
- \\software3.ncsu.edu\Microsoft-Office-2010\$ (Hidden Share)

Application: Microsoft Office 2010 (partial features installed)

License: Purchased Software

Installers: 32-bit and 64-bit

Group Names:

- NCSU-EX-Microsoft-Office-2010-v2 (Creation/Testing)
- NCSU-SW-Microsoft-Office-2010-v2 (Production)
- NCSU-DN-Microsoft-Office-2010-v2 (Deny Group/Production)

GPO Names:

- NCSU-EX-Microsoft-Office-2010-v2-x86 (Creation/Testing 32-bit)
- NCSU-EX-Microsoft-Office-2010-v2-x64 (Creation/Testing 64-bit)
- NCSU-SW-Microsoft-Office-2010-v2-x86 (Production 32-bit)
- NCSU-SW-Microsoft-Office-2010-v2-x64 (Production 64-bit)

Folder Name: Microsoft-Office-2010-v2

Paths:

- \\wolftech.ad.ncsu.edu\software\Microsoft-Office-2010-v2 (DFS)
- \\software1.ncsu.edu\Microsoft-Office-2010-v2\$ (Hidden Share)
- \\software2.ncsu.edu\Microsoft-Office-2010-v2\$ (Hidden Share)

WolfTech AD Software Life Cycle

(Proposed 6/18/2010)

Items in italics are comments and not part of the document.

Overview

The software life cycle will consist of the following major stages:

- Software Request
- Packager Acknowledgement
- Package Creation and Provisioning
- General Testing
- Production
- Retirement and Cleanup

Additional stages:

- Post-production problem reporting/resolution

Software Request

The initial request for the software should to have the following information *(some of this is taken from <http://www.ncsu.edu/software>):*

- Software Vendor Name
- Application Name
- Application Version
- Product Web Site
- Person making the request, including contact info.
- Date software requested to be available by
- Date request submitted
- What does this software replace if anything? (an older version, or another software product?)
- Comments: Benefit to NCSU, who will use it, how will it be used, etc.
- Existing Remedy Call Number *(If not should there be one created?)*
- License/Media information (freeware, site license, etc.)

Some sort of notification should take place to let app packagers know about the new request. RSS feed, email to list, Remedy notification, etc.

Packager Acknowledgement

An application packager will take ownership of the software request:

- Packager provides an estimated completion date
- Userid of packager is recorded
- Time stamp of when acknowledged is recorded
- Remedy call owned to packager

Package Creation and Provisioning

- File Space Provisioned
 - Folder/Share/DFS link created based on approved naming conventions
 - NTFS permissions assigned with full control to the packager's .admin account
- MSI/MST Creation.
 - Packager gets license information and verifies SW/FW status
 - Packager determines the scope (top level OU) of the software package
 - Packager determines if additional GPOs with WMI filters are needed and how many
 - Packager determines if any comments need to be added to the description for the software group
- Software Group Provisioned
 - Provisioned as an "EX" group
 - Software group assigned NTFS permissions with read only access to the file space
- Group Policies Provisioned and Edited
 - Authenticated Users removed from filter, software group added
 - Not linked in by default, packager links to his/her test OU
 - WMI filter applied if applicable
 - Packager does some initial testing (verify that the install works and is configured as expected)

General Testing

- Policies linked at departmentally designated Test OUs
- Announcement of test package availability sent to AD list (or app test list?)
- Testing guidelines:
 - Functionality should be tested by actual users, not just OU admins
 - Should be tested on all supported OSES/architectures
 - Should be tested as non-admin user on local workstation
 - Should be tested with "always install elevated" disabled
 - Test results from each tester should be recorded through an approved system. (*remedy? something else?*)
- Review of testing results
 - Ready for production or needs more testing?
 - **Who has the authority/responsibility to review and decide this?**

Production

- Deny group created
- Software group renamed from EX to SW or FW
- All links removed
- Group policy and file space rights removed, packager will no longer have edit capability
- SW/FW/DN groups get appropriate rights/filter added back to policy and file space
- Announcement of production package availability sent to AD list

Retirement and Cleanup

- Reasons for retirement:
 - No longer secure - retirement required for security reasons
 - No longer licensed - retirement required for compliance reasons
 - Support issues - unable to support older versions
 - MATLAB is an example where multiple versions may need to continue to be supported
 - Full retirement needed or demote to production association at a lower OU?
 - Steps:
 - Confirm that the software group is empty, if necessary contact OU admins about emptying subgroups
 - Exclude from further group replication (*how?*), delete empty software subgroups
 - Inventory reporting, confirm uninstalls, need to allow some time for off campus machines to uninstall before removing GPO and files.
 - Archive files and decommission file space
 - Delete GPO
 - Delete software group
 - Delete software groups
-

Post-production problem reporting/resolution

- How severe is the problem?
- For Minor Changes:
 - Changes to MSI or MST are not a minor changes once app is in production (don't force a reinstall)
 - Checkout process for making changes
 - Backup created of GPO and filespace on checkout before rights are granted
- Examples of minor changes:
 - License update - file space rights can be granted for update, files outside of MSI/MST can be modified as necessary to update license.
 - Firewall rules (should have been caught in testing)
 - Change to an admin template, or GPP item
- Major Changes, including any that modify the MSI or MST, require a new package