Windows Enterprise Announcement

June 5, 2013 – Domain Controller Upgrades Resume (RHEL5, RHEL6, NFS4, and AFS Implications) [Revised]

[Note – This is a revised update schedule following the delay of the WINDC3 upgrade previously scheduled for June 4]

ITS will continue converting the domain controllers to Windows Server 2008 R2 starting June 11, 2013. This will move the remaining domain controllers to Windows Server 2008 R2 (a 64-bit operating system). The first domain controller converted was WINDC5 (on January 8, 2013).   The conversion of the remaining domain controllers will start June 11. The current schedule is:

WINDC3 (129.186.78.28)   - June 11, 2013
WINDC2 (129.186.6.2)   - June 18, 2013
WINDC1 (129.186.6.1)   - July 9, 2013
WINDC4 (129.186.124.249) - SEE LAST SECTION!

During an upgrade the domain controller will not be available for several hours starting about 8:00 AM. Most users will not notice the outage of one domain controller. Windows domain member systems will automatically fail over to one of the four remaining domain controllers. However, if you have systems that will not fail over and are pointed to a domain controller being upgraded you will want to change that prior to the upgrade date.

===== IMPORTANT RHEL5 and NFS4 IMPLICATIONS =====

Mounting and accessing the NFS4 file systems (e.g. CyFiles, OrgFiles) on RHEL5 boxes joined to ISU Active Directory is not supported by domain controllers running Windows Server 2008 R2. Apparently RHEL5 systems request a ticket with the encryption type no longer supported by the Kerberos servers running on Server 2008 R2. To the best of our knowledge, the only solution to this issue is to upgrade to RHEL6. As the upgrades progress, excluding the upgraded domain controllers from the lists in /etc/krb5.conf and /etc/sssd/sssd.conf files will TEMPORARILY solve the issue (SEE LAST SECTION!).

===== IMPORTANT RHEL6 IMPLICATIONS =====

The AES encryption types need to be added to the /etc/krb5.conf to allow the encryption types supported by the new Kerberos servers running on Server 2008 R2:

        default_tgs_enctypes = aes256-cts aes128-cts rc4-hmac des-cbc-crc des-cbc-md5
        default_tkt_enctypes = aes256-cts aes128-cts rc4-hmac des-cbc-crc des-cbc-md5
        permitted_enctypes = aes256-cts aes128-cts rc4-hmac des-cbc-crc des-cbc-md5

===== IMPORTANT AFS IMPLICATIONS =====

These upgrades have important implications if you use AFS and get access tokens from the Windows Domain Controllers. See the Announcements section in the meeting notes for the April 12 WinAdmin meeting here:
http://www.tech.its.iastate.edu/windows/admin/WinAdmin.2013.04.12.pdf

===== **WINDC4 UPGRADE** =====

WINDC4 (129.186.124.249) will be a critical upgrade to the systems with implications listed above. If the above upgrades/changes have not been completed on the day WINDC4 is upgraded service **OUTAGES WILL OCCUR**. Currently ITS is planning a "test day" when WINDC4 will be removed from service for several hours. This will provide an indication of any systems that still need upgrades/changes. Currently this test day is set for August 14, 2013. After the temporary WINDC4 outage it will be brought back (as the same 32-bit OS with no changes).

ITS currently plans to upgrade WINDC4 PERMANENTLY on January 21, 2014. This means all systems with the implications above MUST be upgraded/changed by that date.

===== **QUESTIONS/COMMENTS/CONCERNS** =====

ITS will continue to provide updated announcements on this upgrade via the CCSG, WinAdmin, and MacOSX mailing lists and Critical Event Log as the appropriate. Questions/comments/concerns can be directed to the Network Infrastructure, Authorization & Directory Services group at niads@iastate.edu