Windows Enterprise Announcement

July 17, 2013 – WINDC4 Unavailable 2013-08-14 (IMPORTANT RHEL5, RHEL6, NFS4, and AFS Implications)

[Updated August 7, 2013 – Starting time change from 8:00 AM to 7:00 AM]

ITS will remove WINDC4 (windc4.iastate.edu, 129.186.124.249) from service for one day on August 14, 2013. WINDC4 is the last remaining domain controller running a 32-bit operating system. WINDC4 will be unavailable starting at about 7:00 AM for most of the day.

The purpose of this outage is to TEMPORARILY remove the last 32-bit domain controller from service for one day. This will provide an indication of any RHEL5, RHEL6, NFS4, and AFS systems that still need upgrades/changes (see systems with implications below). After the temporary WINDC4 outage it will be brought back (as the same 32-bit OS with no changes). Managers of systems which saw an outage should immediately begin dealing with the issues by upgrading or reconfiguring.

ITS currently plans to upgrade WINDC4 to a 64-bit operating system on January 21, 2014. This means all systems with the implications listed below MUST be upgraded/reconfigured by that date or **outages will occur**.

During this one day test other systems should not be affected. 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 WINDC4 you will want to change that prior to August 14, 2013.

===== 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. Systems with only WINDC4 in the lists in /etc/krb5.conf and /etc/sssd/sssd.conf files will have service outages on August 14, 2014 and after January 21, 2014 (SEE FIRST 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

===== 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