

Windows Enterprise Announcement

April 12, 2013 – Enterprise Domain Controller Upgrades Continue (Important AFS Implications)

The Windows Enterprise domain controller upgrade project will be resuming May 16 (after grade submission for the current semester). It is hoped to be complete by mid-June. These upgrades were first discussed in the September 2012 WinAdmin meeting. See the meeting notes here:

<http://www.tech.its.iastate.edu/windows/admin/WinAdmin.2012.09.14.pdf>

The first upgrade to WINDC5 happened January 8, 2013. However, after this upgrade it was discovered that the DES encryption type was no longer enabled by Microsoft on Windows Server 2008 R2 (the new OS for the domain controllers). This caused a major problem for AFS clients which use Windows Active Directory Kerberos for authentication. AFS users of the systems pointing at WINDC5 could no longer acquire DES encryption type based AFS tokens. An attempt to enable DES on WINDC5 resulted in many problems with other file servers in the domain (most notably CyFiles and any Windows Server 2003 system). Further domain controller upgrades were placed on hold while the issue was researched.

At this time it has been decided a solution cannot be found for AFS and that the domain controller upgrades can proceed. **It is important to note that once all five domain controllers are at the Windows Server 2008 R2 OS level AFS tokens retrieved from the Windows Enterprise Domain can no longer be used.**

Specifically, Kerberos tickets requiring the encryption types des-cbc-crc will no longer be available. For additional information see the section "Configure Kerberos" at:

<http://www.tech.its.iastate.edu/windows/admin/Rhel6-AD-samba-winbind-keytab.pdf>

Very soon systems using AFS will have no choice but to be configured to get tokens from the old MIT-style Kerberos KDCs. Concerns and questions about this change can be directed to John Hascall [ITSYS] at john@iastate.edu.