Windows Administrators Meeting
May 8, 2009
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- Network cleanup Monday, May 11. Off-campus WINS addresses will be flushed (this is a yearly event).
- Windows 7 and Windows Server 2008 R2 release candidates are available for public testing.

Windows AFS client MUST use KfW [Pruski]

Current versions of Windows OpenAFS use Kerbero-5 credentials only if Kerberos-for-Windows (KfW) is installed. If KfW is NOT installed OpenAFS reverts to using the old Kerberos-4 credentials. This is definitely not recommended in our environment.

ITS publicly announced that Kerberos-4 support was discontinued May 15, 2008. Since that time the Kerberos-4 servers have remained present to allow additional time for some OpenAFS clients to perform their upgrades. Unfortunately some Windows system managers have even recently installed OpenAFS directly from openafs.org without knowing they needed to install the ISU KfW components.

The resolution to the problem is to make sure KfW is installed on any system running OpenAFS (and make sure the OpenAFS version is current, too). KfW is part of a normal Scout install of OpenAFS, so in general Scout-installed OpenAFS systems should be OK. If you do NOT have KfW installed on a Windows system using OpenAFS then you should it install it from the components on www.sitelicensed.iastate.edu

ITS is collecting the IP numbers of systems connecting to the Kerberos-4 servers and will be contacting those system owners who are not using Kerberos-5 in the near future.

IE8 Rollout by Microsoft [Kunz]

Steve Kunz [ITSYS] reminded everyone that Microsoft continues the world-wide rollout of IE8 via Microsoft/Windows Update. Most ISU applications function with IE8 just fine.

WebCT may produce warning messages noting IE8 is an unsupported browser. Since the update of student systems to IE8 is largely out of our control, there is little we can do to prevent students from installing IE8 except via warning notices. WebCT customer support continues to say they will have a version certified for IE8 out “this

summer". It is anticipated that ITS will have that version available (provided it comes out in a timely manner) prior to the start of fall classes.

IT admins can block Microsoft/Windows Update from delivering IE8 using a GPO if they so choose. It won't block WSUS updates from sus.iastate.edu (or any other WSUS server). IE8 is expected to be released by Microsoft to the WSUS server in July 2009. ITS currently intends to allow this update to "auto-approve" when it arrives. A GPO has been provided by Josh Klesel [ENGR] named "IASTATE_IE8_Blocker _5-5-09" should other departments wish to link to it (or use it as a model for their own GPO).

Windows Server 2008 DCs - Summer Rollout Schedule [Kunz & Pruski]

The upgrade of the Windows Enterprise domain controllers (WINDC1, WINDC2, WINDC3, WINDC4) begins with the end of the Spring 2009 semester. The upgrade involves replacing all four production domain controllers with new hardware running Windows Server 2008 (the current DCs run Windows Server 2003 R2 and have been in service since summer of 2003).

Advance TEMPORARY DC for Testing

The Enterprise Admins anticipate few problems with this upgrade. However, as with all Microsoft upgrades there is a focus on "enhanced security" which can affect the wide mix of third party (and older Microsoft) software present in our environment. To allow IT admins to confirm there are no issues with their particular software ITS will offer a fifth TEMPORARY domain controller running on Windows Server 2008 in advance of upgrading any current production DC. This temporary DC will be in place several weeks and will have an LDAPS certificate installed. The sole purpose of this DC will be to allow IT admins with SAMBA, Moodle, Macintosh, and other apps using AD for LDAPS searches and authentication to test and verify their systems will work when WINDC1-4 undergo upgrades at a later date. The temporary DC will be called "WINDC1A" (windc1a.iastate.edu - 129.186.6.7) and will be available sometime on May 18 (watch for further announcements).

IMPORTANT! The hardware to run the temporary WINDC1A will upgrade WINDC1 (in July). After sufficient testing (and prior to July) WINDC1A will be removed from service and used to upgrade WINDC1 in July. DO NOT configure any systems to permanently use WINDC1A as an authentication/LDAPS search target! Any Microsoft domain members which may be using WINDC1A for authentication will automatically convert to another DC when they detect it gone. Third-party apps typically cannot do this and must be manually configured. The date of the withdrawal of WINDC1A will be announced at a later date.

Rollout Dates

The upgrade has some firm and some tentative dates at this point. It will proceed in the following steps on the following dates:

* May 14, 2009 (Thu)
  - Schema updates for W2K8 DCs
  - Forwarding of two new DNS Zones to DC DNS
    (DomainDNSZones & ForestDNSZones)

* May 18 (Mon)
  - TEMPORARY Test DC (WINDC1A) introduced
    (For public testing of 3rd party apps)

* May 27 (Wed)
  - Upgrade WINDC4

* June 9 (Tue)
  - Upgrade WINDC3

* June 23+ (Tue)
  - Upgrade WINDC2

* July 7+ (Tue)
  - Upgrade WINDC1

Send comments/questions/concerns to the Windows Enterprise Admins at its-ad-admins@iastate.edu

Using Terminal Services in the Enterprise Domain [Pruski]

Beata Pruski [ITSYS] talked about Windows Server "Terminal Services" ("TS") in the Windows Enterprise domain. Several colleges/departments have asked questions and made requests over the past months as they move toward more terminal servers in our environment. ITS is publishing the current recommendations after working with several departments.

Current Terminal Services farms (using the Windows Server 2008 Terminal Services environment) expect Terminal Services to be administered and managed at a domain/forest level from a "central services" standpoint. For example, when configuring a domain-member Windows Server 2008 Terminal Services License Server it defaults to a "scope" of "domain/forest". Such a license server needs Enterprise Admin privileges to install (which OU admins will not have). More importantly, according to our current licensing structure such a license server would require a Terminal Services Client Access License (TS CAL) for all users/devices in our domain. The cost under our current licensing structure would be very large. In addition, current TS license servers cannot compartmentalize the licenses held on it, serving out only licenses purchased by each department to that department's systems. All TS CALs go into a common first-come-first-served pool on each License Server. This model does not meet with ISU's distributed management environment.

Another component of a Windows Server 2008 TS farm is a "session broker". This service performs "load balancing" on TS farms. Some departments have asked if ITS would run a central session broker for all TS farms. Unfortunately, a session broker for a farm requires that all the TS servers have the SAME software environment. Again, this does not match our distributed management structure due to the varied software needs of the IT structure at ISU.

The current model for Terminal Services at ISU is for each department to run and manage their own TS license server (purchasing their own TS CALs), broker, and server farm. IT is composing a document outlining this model which will be available on the TechNotes and TechWiki sites. Contact Beata Pruski [ITSYS] at bapruski@iastate.edu for comments/questions.

Open Discussion

Wayne Hauber [ITSEC] talked about a recent botnet news story relating how a university security team had hijacked a large botnet and used the control structure to analyze the extent of world-wide compromised systems and accounts. The numbers were staggering.

Steve Kunz [ITSYS] mentioned that Microsoft had laid off (in their latest round of budget cuts) Steve Riley. Mr. Riley was one of their most noted security experts. We hope they know what they are doing.

Meeting Adjourned (9:45)

Next meeting is scheduled for June 12.