IOWA STATE UNIVERSITY
IT Services Technical Notes
IT

Windows Administrators Meeting

April 12, 2013

Notes (by Steve Kunz, Darrin Fischer, Darin Dugan, Tracy Di Marco White [ITSYS])

Meeting Started (9:00)

Announcements

- Domain Controller Status: Steve Kunz [ITSYS] commented that the domain controllers have been stabile since March 20. Whatever was happening has stopped. ITS will probably close the Microsoft Premier Support Case next week and remove the CEL.

- Demise of the ITS Computer Inspector: As first announced in the Tuesday SecSIG meeting, the ITS Computer Inspector will no longer be required for NetReg registrations (mostly in the residence halls) in the near future. No formal date has been established but it will certainly be decommissioned by fall semester 2013. The main reason is that some major anti-virus products (Symantec and Webroot are two) view Inspector as malware and will not allow it to operate. Since no circumvention has been found Inspector will be decommissioned.

- DC Upgrades Continue After May 16 (AFS implications): Steve Kunz [ITSYS] announced that 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 in January 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.

- Windows Enterprise Administrators Changes: Steve Kunz [ITSYS] announced some changes in the ITS staff assigned as Windows Enterprise Administrators. Mark Bland [ITSYS] and Darin Dugan [ITSYS] are coming on board as new Windows Enterprise Administrators next week. Steve Kunz [ITSYS] and Vince Oliver [ITSYS] will be transitioning out of their Windows Enterprise Admin duties over time. Beata Pruski [ITSYS] will remain as Senior Windows Enterprise Admin.

SCCM 2012 – Darrin Fischer [ITSYS]

SCCM 2012 Servers are up and running and available. They consist of all virtual servers including:

- CAS (Central Administration Site)(itssccm12cas)
- Primary Site Server (itssccm12)
- Database Server (itssccm12db)

ITS has migrated from SCCM 2007 to SCCM 2012. Other areas are either in the process of migrating or have test collections setup on the server.

Some Major Changes:

1. New Configuration Manager Console
2. Improved distributed rights. Now has security based roles such as:
   a. Application Manager
   b. OS Deployment Manager
   c. Asset Manager
   d. Remote Tools Operator
   e. Endpoint Protection Manager
   f. Many more…
3. Scope based:
   a. Can now set perms on applications, packages, and other components of SCCM
   b. Will allow departments to restrict their apps to be seen only by themselves.
   c. Other advantages
4. System Center Endpoint Protection (SCEP) replaces Forefront Endpoint Protection (FEP). SCEP is Windows 8 compatible.
5. Hierarchy of collections no longer exists like in SCCM 2007 (helps prevent accidental sub-collection package/application distribution).
6. Not just packages, now has applications which you can get more granular with criteria based app deployment based off of MSIs.
7. WSUS role installed on server
8. SQL reporting services

9. Enhanced Monitoring and Alerts
10. We have the Casper plug-in installed and configured so we are getting Mac data from Casper into SCCM's database.
11. There are updated Remote Tools

Migration plan for other areas currently on SCCM 2007:

- ITS would like to decommission the SCCM 2007 server by the end of August of this year.
- ITS welcomes new departments/colleges wanting to get set up on SCCM 2012.
- To get set up on SCCM 2012, please give us the root OU you want collections based on and either the user(s) or AD security group that should have access. Send email to sccmrootadmins@iastate.edu.

ITS will do a demo in either an upcoming WinAdmin meeting or schedule a separate meeting.

Terminal Services License Servers – Darin Dugan [ITSYS]

Darin Dugan [ITSYS] talked about Terminal Services license server support. This topic was discussed at the November 2012 WinAdmin meeting (see meeting notes here: http://www.tech.its.iastate.edu/windows/admin/WinAdmin.2012.11.09.pdf). Referring to those notes "Scenario 3" has been chosen ("Departmental license servers: Any department can set up and run a license server").

For compliance auditing, departmental license servers issuing per-user CALs can be added to the domain "Terminal Server License Servers" group on request (send email to its-ad-admins@iastate.edu). Having your departmental license server as a member of this group allows it to update the per-user CALs for any user object in the domain.

An ACL change will be coming for certain user objects to make per-user license tracking possible domain-wide. User objects created prior to the introduction of Windows Server 2008 domain controllers need to have their security permissions altered so the servers in the "Terminal Server License Servers" group are able to log their usage. This change will be lab-tested soon and an announcement made when the change will happen. This change will require no action on IT admins' part and simply corrects the per-user CAL recording on the user object.

Dugan has updated the TechNotes documentation for Terminal Services (a.k.a. Remote Desktop Services) here:
http://www.tech.its.iastate.edu/windows/admin/W2K8TermServ.pdf

Dugan also noted that Windows Server 2012 Remote Desktop Licensing is not significantly different from Windows Server 2008 R2.

Proposed Changes to DNS Service for Off-campus Users – Tracy Di Marco White [ITSYS]

Tracy Di Marco White presented proposed changes in the way DNS servers can be accessed from off-campus. Iowa State University DNS servers have participated in DDoS (Distributed Denial of Service) attacks against other systems on the Internet in the recent past. These attacks do not originate on the DNS servers at ISU, but the ISU DNS servers serve as a middle-man in the attack, amplifying a flood of DNS requests from an attacker's group of systems through ISU DNS servers forged as if from the victim site. This causes an overload at the victim site receiving the request and a subsequent denial of service.

ISU is being scanned for recursive DNS servers by two groups – the attackers who want to use our servers in attacks and Internet watch-dogs (such as REN-ISAC) who want us to properly configure our DNS services.

There are two things that must be done to eliminate ISU DNS servers from participating in the attack. First, ISU DNS servers should NOT do recursive lookups unless absolutely necessary. A recursive lookup occurs when the local DNS service cannot resolve the address requested and must refer it to another site. Second, port 53 (the DNS port) must be blocked at the campus border so that only the main DNS servers (DNS-<n>.iastate.edu) are open to the internet and rate-limited (to reduce the efficiency of any attack).

A timeline for these changes has yet to be determined, though ITS intends to act as quickly as possible to aid in the reduction of these attacks. Watch for further information the main public mailing lists and meetings (CCSG, WinAdmin, etc.).

It should be noted that DNS service is running on all five domain controllers. This service is needed to be able to provide DNS resolution for critical domain services like LDAP, the KDC, etc. By default this DNS service is configured to do recursive lookups. However, this is unnecessary and recursion will be turned off May 16, 2013. If you have correctly configured your systems to point to the main NS-<n>.iastate.edu servers on the IP configuration tab the change will have no impact on you.

Open Discussion

The question was asked whether there was another product departments could use to perform similar functions of the ITS Computer Inspector product. Wayne Hauber [ITSEC] commented that while there are a few other "pay for" products ITS has not pursued purchasing any as of yet.

Meeting Adjourned (10:00)

Next meeting is scheduled for May 10 (provided a sufficient agenda exists).