

**Iowa State University  
Information Technology Services**

**Windows Administrators Meeting**

August 10, 2007

Notes (taken by Steve Kunz)

**Meeting Started (9:00)**

**Announcements**

- The Enterprise WSUS server was upgraded from WSUS 2.0 to version WSUS 3.0 on July 31. No problems were encountered.
- Be aware of the "Google Desktop and Exchange Issue". "Google Desktop" provides an "indexing service" to anything a user uses on a local system – including network file shares and email stored on an Exchange server. This indexing activity can cause considerable load on an Exchange server. Vince Oliver [ITSYS] posted good information on this issue to the Exchange Administrators ("exchadmin") mail list on August 8. Text of that post is available at:  
<http://tech.ait.iastate.edu/win2000/admin/GoogleDesktop.pdf>
- Be aware of the latest BackupExec "high severity" security advisory (SYM07-015). Mike Long [CARD] posted information on this issue to the WinAdmin and SecSig mailing lists on July 13. Get the latest from Symantec here:  
<http://entsupport.symantec.com/docs/289731>  
Wayne Hauber [ITSEC] commented that this issue has moved from being a "denial of service" issue to a "full exploit".

**Imaging Windows Systems with OpenAFS Installed – Kunz [ITS]**

ITS AFS servers had a "severe load issue" on Tuesday, August 7. This was caused by improperly imaged systems in one department. The load on the AFS servers resulted in those client systems being blocked from AFS access while ITS worked with the departmental IT admin to correct the problem.

The AFS "Release Notes" documentation includes information on properly imaging systems with SysPrep, but it is somewhat "buried". The important information has been extracted into a new ITS Technical Note titled "Imaging Systems That Use OpenAFS". This document is available in the "OU Administrator Support" area under the "Tips for Deploying Systems and Software" section. A direct link to the document is here:

[http://tech.ait.iastate.edu/win2000/admin/Imaging\\_OpenAFS.pdf](http://tech.ait.iastate.edu/win2000/admin/Imaging_OpenAFS.pdf)

Jim Wellman [AER E] asked if there was any way to detect whether an image was correctly created "after the fact". Kunz said he would investigate. [Information since the meeting: One method may be to look at imaged systems and see if the AFSCache file is absent before AFS is used the first time. Typically this file is in WINDOWS\TEMP\AFSCache).

**Shutting Down LDAP Simple Binds on Enterprise AD – Kunz [ITS]**

ITS is in the process of shutting down “simple LDAP binds” to the Enterprise Active Directory domain controllers. A “simple LDAP bind” is the “minimum security” bind type according to LDAP standards and is “clear text password transmission”.

Modern Windows systems never use “simple LDAP binds” to communicate with AD. Secure (kerberos) authentication is always used. However, some third-party software (including “open source” software) may use “simple LDAP binds”. This software will cease functioning when ITS closes down “simple LDAP bind” authentication. If you are aware you are using such software (pointing to WINDC1-4 on LDAP port 389) you should contact Steve Kunz as soon as possible ([skunz@istate.edu](mailto:skunz@istate.edu)).

The more secure alternative to “simple LDAP binds” will be a certificate-based “LDAPS” authentication model. ITS will work with any current “simple LDAP bind” users to transition to the new LDAPS method. “Step 1” in this process is this “awareness” announcement about the intent of ITS to shut down this clear-text authentication. “Step 2” will be ITS analyzing the “simple LDAP bind” traffic to the domain controllers to determine who is using the service in this way and contact them. “Step 3” will be to resolve the issue by working with the IT admins to secure the service. Watch for more information in the WinAdmin forums in the future.

## **Open Discussion**

Jim Wellman [AER E] asked about ITS Exchange services and “Out of Office Assistant” mail loops. Jim said they have encountered issues with a setting not being set which is supposed to allow only one “out of office” email a day being sent. This caused a “mail loop” when two “out of office” Exchange recipients bounced back to each other. Frank Poduska [ITCSV] will follow up and work with ITS Exchange staff and Jim Wellman. This is only an issue between two “ISU Exchange Org” mail users. POP3 users and the “vacation message” facility are not affected (the ASW “vacation message” facility does not deal with Exchange-to-Exchange intra-org email).

Darin Dugan [C EXT] commented that a related issue with the ASW “vacation message” facility is that forwarded POP3 mail cannot use the “vacation message” facility. ITS staff remarked this is a known limitation of that service (probably by design).

David Orman [CNDE] asked what people were using to deploy large numbers of Windows Vista systems (or IF they were deploying large numbers of Windows Vista systems). Darin Dugan [C EXT] said they were using “workbench tools” to build unattended install files for remote manual DVD installs at their field offices.

Frank Poduska [ITCSV] asked if anyone was deploying Windows Vista on a large scale. Of those attending, only Darin Dugan [C EXT] said Extension was deploying over 100 systems. [Additional information since the meeting: ITS is seeing about 240 Windows Vista systems contacting the KMS server and a little over 100 Windows Vista systems using Scout for software installs at this point. SLK]

Beata Pruski [ITSYS] commented that Dan Carlile [ITCSV] has made “Windows Vista Ultimate” available off the MCA shares. Windows Vista Ultimate cannot be activated via KMS, so you will have to contact Dan directly for a software activation key.

**Meeting Adjourned (10:35)**

Next meeting is scheduled for Sep 14, 2007.