**Windows Administrators Meeting**
September 9, 2005
Notes (taken by Steve Kunz)

## Meeting Started (9:05)

## Announcements

Deb Best is our new Microsoft "Education Account Manager". She is filling Casey Niemann's position. Deb's email address is dbest@microsoft.com .

## Live Communication Server 2005 SP1 (Darin Dugan [CECS])

Darin Dugan [CECS] talked about Extension's "Live Communications Server" project. Live Communication Server is an "enterprise class" service similar to Exchange and SMS.

This product is being discussed as a "departmentally supported" software product. It should not be implied that Live Communication Server is being supported by Information Technology Services as an "ITS offering" (you should not expect help-desk support for product features via the Solution Center, for example). However, other colleges/departments may see similar benefits and be able to use Live Communications Server for their own needs. Collaboration is encouraged.

Live Communications Server (hereafter abbreviated "LCS" in this document) is Microsoft's enterprise real-time communications server. Essentially, LCS is a SIP-compliant server for presence, IM, etc. The principal client application is Office Communicator 2005, a new product to replace Windows Messenger.

Extension plans to use LCS and Communicator immediately for the basic things such as presence, text IM, one to one audio and video, application sharing, file transfers, etc. Presence information is exposed through Office applications such as Outlook, and through SharePoint. Exchange free/busy information is also used to automatically set user status to Away during meetings, etc (for those also using Exchange). Also, instead of adding every user you want to communicate with to your contact list, you can search for users from the GAL. In the longer term, Extension hopes to do more with presence, custom applications using IM, and maybe telephony.

Other departments can put up and manage their own LCS servers. A domain admin must authorize new LCS servers when initially installed, but thereafter it is entirely departmentally managed. Management is segregated by servers you admin and users you "own" in AD. At this point Extension has not considered LCS for users that you don't own (such as students).

There are several LCS settings that can either be set globally or per server, such as archiving and encryption. The assumption is that nothing (or almost nothing) will be set globally, so that each department can have full control over their own server.

To participate in the LCS environment would require the normal staff, hardware, software, and licensing issues. In terms of staff time, Extension anticipates very little work being needed after initial installation. Users are "LCS enabled" in AD Users &

Computers, and that's mostly it. A single LCS server may meet a departments needs. Microsoft contends that a single LCS server will handle 10-15 thousand users.

There are LCS licensing issues. People wanting to bring up their own LCS server would need a Windows 2003 OS license, an LCS Server license, plus per-user CALs. The LCS 2005 Standard Edition server license thru the MCA server's option is something like $125/year. CALs should be $1.89/user. Telephony CALs are an additional $1.89/user. Public IM connectivity to Yahoo, AIM and MSN are available, but the licensing and costs are not yet known.

Extension and ITS still need to deploy LCS in a test lab to verify that management works as expected, and that there are no surprises. LCS does require some schema extensions.

There are also additional LCS server roles that need to be investigated and fleshed out, including a front-end type server, which directs clients to the correct LCS server, and an Access Proxy, which allows LCS use outside ISU without VPN, and federation with other LCS organizations.

Bill Frazier [ITS] asked about security implications of a new Microsoft network product.

More information:
www.microsoft.com/office/livecomm/prodinfo/overview.mspx

Darin Dugan can be reached via email at dddugan@iastate.edu .

**Kerberos for Windows (B. Pruski [ITS])**

Beata Pruski [ITS] talked about the new Windows Kerberos libraries that are nearing production status. The new libraries come from MIT and are called "KFW" (Kerberos for Windows). These libraries are tightly integrated with the newer versions of OpenAFS and provide native Kerberos 5 authentication (with no "Kerberos 4 translation" process). Beata has also written a new "Kerberos Integrated Login" package using the new libraries. One key benefit is that there are no more "blue screen pauses" that started cropping up on some XP systems after SP2 was applied.

ITS has been using these new products internally for some time. Recently a few other departments volunteered to test the new KFW libraries and they encountered few problems. At this point ITS is willing to expand its "pre-production" testing audience within the WinAdmin group. Contact Beata at bapruski@iastate.edu if you want to participate.

**LANMAN and NTLM (S. Kunz [ITS])**

Steve Kunz [ITS] spoke of his perennial concern about LANMAN and NTLM authentication protocols being allowed in communications with the Enterprise domain controllers. Advice from security experts is always that these protocols should be disabled (allowing only NTLMv2 and Kerberos for authentication). For

practical purposes these older protocols are "clear text" in terms of password security over the network. In the past various services offered by departments (such as "SNAP servers" and older SAMBA servers) required LANMAN or NTLM. Kunz asked the question again as to whether or not anyone was aware of the need for these old protocols in our current environment. Nobody at the meeting knew of any.

Kunz said the next step is to announce a proposal to the WinAdmin mailing list on disabling the LANMAN and NTLM protocols for domain authentication. Should there be no "show stopper" needs a date (in the future) will be set and we will proceed. Email skunz@iastate.edu if you have any concerns about this issue (or watch for the post in the WinAdmin mailing list and respond to that).

**Open Discussion**

- Steve Kunz [ITS] mentioned that a few departments are beginning to experiment with Microsoft's "Sharepoint Portal" services. This is another "departmentally supported" product at this point. Kunz asked if anyone had any ideas for "shared support" of such products (since there may not be a great deal of knowledge at the Solution Center for such products). Are email lists OK? Web-pages? Blogs?

- Beata Pruski [ITS] mentioned she developed a new "attach" command for Windows systems. This command-line executable lets you attach AFS file systems by supplying their name (not mount-point) and a drive letter to map it to. It can be very handy in login scripts, etc.

- Chris Thach [CIRAS] asked about the status of the PKI infrastructure and a Windows digital certificate server. Kunz indicated he takes every opportunity to remind ITS people that this is a needed service.

- Dave Orman [CNDE] asked about support for "Services for Unix". Key to this support is the inclusion of Unix-affiliated fields in an LDAP server (Active Directory in the case of Microsoft's product). Bill Frazier [ITS] stated that this may be similar to the needs of the Macintosh community which had extensions applied to the main LDAP server. Further research will be done on this (probably involving others).

**Meeting Adjourned (about 9:45)**

Next meeting is scheduled October 14