

Re: Help me replace some Windows installations

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.setup/2004-09/0453.html>

From: ZnU (znu_at_acedsl.com)

Date: 09/14/04

Date: Mon, 13 Sep 2004 19:42:35 -0400

In article <2qldjqF10grg0U1@uni-berlin.de>,
Abdullah Ramazanoglu <abdullah@ramazanoglu.tr> wrote:

> begin ZnU <znu@acedsl.com> dedi ki:
> > In article <hs9fI2-025.ln1@triangulo.it.uc3m.es>,
> > ptb@oboe.it.uc3m.es (P.T. Breuer) wrote:
> >> ZnU <znu@acedsl.com> wrote:
> --8<--
>
> Again set follow up to c.o.l.misc
>
> > Look, I don't understand what the miscommunication is here.
> > Basically, what I want to do, is let a user log in and have
> > appropriate access to his home directory, and appropriate lack of
> > access to the home directories of other users. The way Windows and
> > OS X handle this is by mounting home directories as share points
> > using the authentication information for the user logging in on
> > each machine. In other words, if I log in as 'znu' on Client-1,
> > Client-1 logs into the file server using the 'znu' account, and the
> > 'Users' share is mounted with the privileges defined for 'znu' on
> > the server.
>
> > Possible with untrusted clients in SMB, and trusted clients in NFS.
>
> > With NFS, my understanding is that I'd create a system-wide entry
> > to mount the 'Users' share at, say, /home. If I did that, I'd have
> > to grant the client full read-write access on the entire share,
> > because it has to be able to grant the appropriate access to any
> > user who might sit down and log in, and that potentially requires
> > being able to read from and write to any home directory. I then
> > have to trust the client to make sure that user A doesn't delete
> > files from user B's home directory or whatever. I can't necessarily
> > trust every client that might be connected to this network.
>
> > Subtly wrong. You have to trust the *administrator* of the client
> > machines. There's a misconception of "trusting a user on the client"
> > and "trusting the administrator of the client". If you administer
> > both clients and servers, then there's no risk of user X accessing

> *home of user Y.*

It's hard to totally lock down machines that untrusted users have physical access to. It's even harder to lock down an entire physical network. What if someone shows up and plugs in their laptop? I really don't want to have to deal with all of these issues. That's what I was getting at.

> *It's because with NFS (plain NFS) granting access to a remote machine just enables NFS sharing for that machine in general, but it doesn't allow for *any* user on the client to access any exported directory. Still, user ABC on client, accesses to server with rights of the user ABC on server. This scheme is only risky if someone can install his own Linux client and, being root of his own machine, create arbitrary user accounts on this client, which enables him to access to NFS server as any user he chooses. Plain NFS is to be used in trusted-administrator environments, historically. If you can't trust the admin of a remote machine, then you don't grant NFS access to that machine. If you can't trust your LAN environment, then don't use plain NFS. Either use some sort of secured NFS, like kerberized NFS which Peter already told you about, or use SMB for Linux to Linux shares. NFS is not Linux, like SMB is not Windows. They're just RFC'ed file sharing protocols.*

>
>>> *OpenDirectory is basically OpenLDAP with an Apple schema that provides everything OS X needs. I *think* this schema is a superset of RFC 2307 (which is what I'd want for Linux clients, right?), but it's hard to*
>>>
>>> *I have no idea. If you have an ldap server, then linux can use it for authentication. It's a question of putting a few entries in the pam.d files, and arranging that nsswitch.conf is rigged to refer libc getpwent through ldap for the passwords.*
>>
>> *See, this is the kind of thing that makes people say Linux is not ready for prime time.*

>
> *You've started this thread with "I've got a chance to replace 30 Windows machines, please help me..." and now you seem to be more interested in making comparisons rather than get help and get going.*

Well, it's a little hard *not* to make comparisons, you know? I mean, this was painless on the other two platforms (I'd never done it before, and I didn't even have to read the docs), and the explanations I'm getting for Linux practically read like geek parody.

> *I don't know what are you after. Just argue for the sake of argument? A cat in the bag? If you are really interested in a solution, then why are you keeping on posting to c.o.l.advocacy, which has nothing to do with your technical questions, and why didn't you replied to my post in c.o.l.misc?*

comp.os.linux.setup: Re: Help me replace some Windows installations

What I was after was some information about getting Linux clients to talk to an OS X Server, or at least some confirmation that somebody else had gotten it to work. Instead people have yelled at me to read somewhat-related documentation that I could have found myself, and have argued with me over my Windows licensing situation.

[snip]

--

"I want to thank my friend, Sen. Bill Frist, for joining us today.... He married a Texas girl, I want you to know. (Laughter.) Karyn is with us. A West Texas girl, just like me."

-- George W. Bush in Nashville, Tenn., May 27, 2004