Re: One login for multiple machines

Source: http://linux.derkeiler.com/Mailing−Lists/Ubuntu/2007−03/msg00691.html

- *From*: "Eric Dunbar" <eric.dunbar@xxxxxxxxx>
- *Date*: Thu, 8 Mar 2007 20:29:12 −0500

On 08/03/07, Joel Bryan Juliano <joelbryan.juliano@xxxxxxxxx> wrote:

> On 3/8/07, H. S. Rai <hardeep.rai@xxxxxxxxx> wrote:
>
> > I am setting up a lab, and proposing to have dual boot, ubuntu and
> > MSXP. For Ubuntu bases setup, I want student should able to sit on any
> > machine, get authenticated from remote server (thus not need to create
> > user on every machine), gets his home directory served from some
> > server, able to run applications from local machine with data accessed
> > and stored from his remote home directory.
> >
> > May you suggest me what need to be installed on Server, and how client
> > need to be configured (may be with some additional softwares.)
> >
> > Simple advise and pointer to article, howto or tutorial will be more
> > than enough.
> >
> > Thanks in advance,
>
> Probably the best solution for that is NIS.

I found two interesting pages on the subject (I'm wanting to play with an automated, seamless network drive, and, separately (for a different network) a centrally−stored login on a Linux server for Windows PCs (the software I want the network to have is Windows (and, Mac)−only).

FYI... I've excerpted some relevant info from two web pages on NIS and LDAP...

http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch30_:_Configuring_NIS

Quick HOWTO : Ch30 : Configuring NIS

Network Information Services (NIS) enables you to create user accounts that can be shared across all systems on your network. The user account is created only on the NIS server. NIS clients download the necessary username and password data from the NIS server to verify

each user login.

An advantage of NIS is that users need to change their passwords on the NIS server only, instead of every system on the network. This makes NIS popular in computer training labs, distributed software development projects or any other situation where groups of people have to share many different computers.

The disadvantages are that NIS doesn't encrypt the username and password information sent to the clients with each login and that all users have access to the encrypted passwords stored on the NIS server. A detailed analysis of NIS security is beyond the scope of this book, but I suggest that you restrict its use to highly secure networks or to networks where access to non−NIS networks is highly restricted.

The Lightweight Directory Access Protocol (LDAP) offers similar features to NIS but has the advantage of supporting encryption without additional software and can support clients across multiple networks without the need for slave servers. It is for this reason that LDAP has become increasingly popular for this type of application. LDAP is discussed in more detail in Chapter 31, "Centralized Logins Using LDAP and RADIUS".

Conclusion

NIS is a very useful tool for centralized login management, but it has two shortcomings: NIS clients are typically limited to Unix or Linux operating systems, and the password information passes over the network unencrypted.

http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch31_:_Centralized_Logins_Using_LDAP

LDAP is rapidly becoming a defacto standard for remote authentication and authorization of users, not only in the realm of Linux, but also in that of Windows where it is a key component of Active Directory. Usage of LDAP is also becoming increasingly widespread in wireless networking systems. For example in hot spots, ISPs will sacrifice data security for the sake of convenience by not using encryption, but will use LDAP to restrict access to the Internet to people who have purchased pre−paid access codes with a predefined lifetime.

Chapter 32, "Controlling Web Access with Squid", covers the use of the Linux Squid application to cache Web content, restrict Web access by the time of day and via password prompts. Although it is beyond the scope of this book, you should know that you can use LDAP can to complement the functionality of Squid in larger implementations.

−−
ubuntu−users mailing list
ubuntu−users@xxxxxxxxxxxxxxx