

## Re: noob on slapd with sasl errors

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2006-09/msg01253.html>

---

- *From:* Zach <[uid000@xxxxxxxxxx](mailto:uid000@xxxxxxxxxx)>
  - *Date:* Tue, 12 Sep 2006 13:06:18 -0400
- 

If I may share advice based on my own trials & tribulations with LDAP authentication:

You've just hit on a major issue. LDAP is a critical technology for people who need network authentication and the current state of documentation for implementing it is depressing. Partly the problem lies in the fact that it is difficult to set bounds around what LDAP does/doesn't/can/can't provide. Although frequently discussed in the context of network authentication, LDAP really is just a protocol used to access a directory of information over a network. In the context of network authentication, the directory contains information about users, credentials (passwords), etc. However the directory can be anything—address book, whatever.

With regards to implementing an LDAP-based network authentication system, there is a lot of mixed, conflicting information out there. Much of it tends to be specific to the author's situation. You really have to sort through it and experiment a few times to get a handle on how the whole thing works to get a feel for what information to discard and what to keep.

Here's some LDAP information on the Debian wiki:  
<http://wiki.debian.org/LDAPAuthentication>

Be warned it's a mess—mostly a collection of resources. It's anything but a walkthrough.

Also, O'Reilly's Linux Server Hacks Volume 2 (<http://tinyurl.com/h9nsg> — not sure if it's available in Germany/Deutsch) has a chapter on using LDAP for Network Authentication. I haven't tried implementing it from that book, but it looks pretty good. It may be worth browsing at a bookstore to see if it looks helpful.

Based on my experience, I would make the following recommendations:

- \*Start with a fresh system. Migrating user/group accounts is possible, but more complicated
- \*Get LDAP going first, then fuss with SSL/TLS
- \*Work with a couple of sacrificial machines, rather than production

## Re: noob on slapd with sasl errors

systems. If you can't spare the machines, give VMWare Server a try. It's free, and Ubuntu runs well on it.

\*Be willing to start over multiple times.

\*When you're configuring slapd, make sure you understand all directives you're using. \*Even if that means running down an explanation one directive at a time. Every directive exists for a reason. What applies to one person's situation may not apply to yours. Only when you understand each and every line in your slapd.conf can you achieve true Zen.

LDAP authentication really isn't all that hard. It's just that you have to have a working vocabulary to make sense of most of the documentation out there. You have to get your hands dirty and break it a few times in order to build a vocabulary.

Good luck

On 9/12/06, Kaiser, Hans <r\_2@xxxxxx> wrote:

> Hello,

I am currently switching dapper to ldap authentication, but after only few steps I have to give up...

I have configured my slapd.conf like it is presented here:  
[http://www.howtoforge.com/linux\\_ldap\\_authentication](http://www.howtoforge.com/linux_ldap_authentication)

I got stuck with the first ldapsearch command.  
ldapsearch -D "cn=Manager,dc=domain,dc=com" -W  
Enter LDAP Password:  
SASL/DIGEST-MD5 authentication started  
ldap\_sasl\_interactive\_bind\_s: Internal (implementation specific) error

(80)

additional info: SASL(-13): user not found: no secret in database

and the log files tells me:  
SASL [conn=1] Failure: no secret in database  
conn=1 op=2 RESULT tag=97 err=80 text=SASL(-13): user not found: no secret in database

Hope someone can help me....

I have no idea how sasl works and why it is needed here, or even more, how to configure it.

regards

Re: noob on slapd with sasl errors

Try adding `-x` to your `ldapsearch` command to use simple authentication instead of SASL, i.e;  
`ldapsearch -x -D "cn=Manager,dc=domain,dc=com" -W`

Thanks, I will try it!  
Anyway is there a howto, which describes the configuration, which is needed to work properly with/without sasl?

--

ubuntu-users mailing list  
ubuntu-users@xxxxxxxxxxxxxxxxxxxxx  
<https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>

--

If you reply to a message I posted in a mailing list thread, There's a chance I may not see your response. Feel free to address me directly in the 'To:', in addition to posting to the list.

--

ubuntu-users mailing list  
ubuntu-users@xxxxxxxxxxxxxxxxxxxxx  
<https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>