

Re: Fedora Core 5 LDAP client authentication problem with Solaris 9 iPlanet LDAP Server

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2006-06/msg03354.html>

- *From:* Nigel Wade <nmw@xxxxxxxxxxxxx>
 - *Date:* Tue, 20 Jun 2006 18:48:39 +0100
-

ay0my wrote:

Hi,

Nigel:

"Look for pam_check_host_attr, pam_groupdn and pam_member_attribute."

These 3 attributes in /etc/ldap.conf are commented out with a #, hence I do not think they are causing the problem.

Yes, I'm pretty sure that's right, they need to be enabled to have any effect.

Can you determine if the system is actually making requests of the LDAP server when a login is attempted? The normal way that authentication is validated is for pam_ldap to attempt to bind to the LDAP server as the user in question, using the supplied password. If the LDAP server isn't configured to allow this type of authentication it will obviously fail.

Is the connection to the LDAP server using SSL? If not, you could use a packet sniffer such as ethereal to capture the packets to the ldap port, and see

One thing has just occurred to me. Does the users home directory exists? IIRC, I've seen "permission denied" when the home directory does not exist.

Gordon:

The /etc/pam.d/system-auth is attached below. Apologize that I do not know what to look for in this file. Thanks for your advise.

```
[root@sspxz1000 pam.d]# cat system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth required pam_env.so
auth sufficient pam_unix.so nullok try_first_pass
auth requisite pam_succeed_if.so uid >= 500 quiet
```

Re: Fedora Core 5 LDAP client authentication problem with Solaris 9 iPlanet LDAP Server

```
auth sufficient pam_ldap.so use_first_pass
auth required pam_deny.so
account required pam_unix.so broken_shadow
account sufficient pam_succeed_if.so uid < 500 quiet
account [default=bad success=ok user_unknown=ignore] pam_ldap.so
account required pam_permit.so
password requisite pam_cracklib.so try_first_pass retry=3
password sufficient pam_unix.so shadow nullok try_first_pass use_authtok
password sufficient pam_ldap.so use_authtok
password required pam_deny.so
session required pam_limits.so
session required pam_unix.so
session optional pam_ldap.so
[root@sspxz100 pam.d]#
```

Regards

This is my system-auth, generated on RHAS 4, which works for authentication against an openldap server:

```
##PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth required /lib/security/$ISA/pam_env.so
auth sufficient /lib/security/$ISA/pam_unix.so likeauth nullok
auth sufficient /lib/security/$ISA/pam_ldap.so use_first_pass
auth required /lib/security/$ISA/pam_deny.so

account required /lib/security/$ISA/pam_unix.so broken_shadow
account sufficient /lib/security/$ISA/pam_localuser.so
account sufficient /lib/security/$ISA/pam_succeed_if.so uid < 100 quiet
account [default=bad success=ok user_unknown=ignore] /lib/security/$ISA/pam_ldap.so
account required /lib/security/$ISA/pam_permit.so

#password requisite /lib/security/$ISA/pam_cracklib.so retry=3
password requisite /lib/security/$ISA/pam_passwdqc.so min=disabled,disabled,12,7,7
password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password sufficient /lib/security/$ISA/pam_ldap.so use_authtok
password required /lib/security/$ISA/pam_deny.so

session required /lib/security/$ISA/pam_limits.so
session required /lib/security/$ISA/pam_unix.so
session optional /lib/security/$ISA/pam_ldap.so
session required /lib/security/$ISA/pam_mkhomedir.so skel=/etc/skel/

--
```

Nigel Wade, System Administrator, Space Plasma Physics Group,

Re: Fedora Core 5 LDAP client authentication problem with Solaris 9 iPlanet LDAP Server

Re: Fedora Core 5 LDAP client authentication problem with Solaris 9 iPlanet LDAP Server

University of Leicester, Leicester, LE1 7RH, UK

E-mail : nmw@xxxxxxxxxxxxx

Phone : +44 (0)116 2523548, Fax : +44 (0)116 2523555

--

fedora-list mailing list

fedora-list@xxxxxxxxxxxxx

To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>