

# Re: LDAP Authentication from Linux

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-04/msg00569.html>

---

- *From:* "Dana Epp [Security MVP]" <[dana@xxxxxxxxxxxx](mailto:dana@xxxxxxxxxxxx)>
  - *Date:* Thu, 3 Apr 2008 13:27:37 -0700
- 

If I recall correctly, doesn't the LDAP module in Apache require a secure connection on most recent Linux systems? Shouldn't that be 'ldaps://'?

Try something like this:

```
<Directory "/var/www/html/wiki">
```

```
AuthType Basic
```

```
AuthBasicProvider ldap
```

```
AuthName "test server"
```

```
AuthLdapAuthoritative on
```

```
AuthLdapEnabled on
```

```
AuthLDAPURL
```

```
"ldaps://ubiq-serv1.companyname.local:389/DC=companyname,DC=local?sAMAccountName?sub?(objectClass=*)"
```

```
AuthLDAPBindDN
```

```
"CN=ldap45457,OU=SBSUsers,OU=Users,OU=Corporate,OU=MyBusiness,DC=companyname,DC=local"
```

```
AuthLDAPBindPassword *****
```

```
require valid-user
```

```
</Directory>
```

I am guessing if it works with a domain admin that maybe SSL isn't required, but I would recommend you do that anyways. You will also notice I set AuthLdapAuthoritative "on" to ensure it fails securely and does not allow any alternate credential check from creeping in and be allowed.

Regards,

Dana Epp [Microsoft Security MVP]

"Adrian Marsh (NNTP)" <[adrian.marsh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:adrian.marsh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:%23eJSPJalIHA.5660@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23eJSPJalIHA.5660@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I've also just tried this:

Moving the ldap45457 user into the same OU as the rest of my normal users, and then changing apache to the below, and also adding "List Contents" Read permissions to that OU, as per what I read here for anonymous access. But still failed.. :(

Re: LDAP Authentication from Linux

[http://www.petri.co.il/anonymous\\_ldap\\_operations\\_in\\_windows\\_2003\\_ad.htm](http://www.petri.co.il/anonymous_ldap_operations_in_windows_2003_ad.htm)

AuthLDAPURL

"ldap://ubiq-serv1.companyname.local:389/OU=SBSUsers,OU=Users,OU=Corporate,DC=companyname,DC=local"

NONE

AuthLDAPBindDN

"CN=ldap45457,OU=SBSUsers,OU=Users,OU=Corporate,OU=MyBusiness,DC=companyname,DC=local"

AuthLDAPBindPassword \*\*\*\*\*

Adrian

Adrian Marsh (NNTP) wrote:

Hi Dana,

I think you're right about the Query privileges. What I would like is a user specifically used for the binding, so restricted in other things. I'm not sure how to set those privileges though. I know that if I change the apache config below to use a Domain Admin account, then all works well.

Heres the Apache config:

```
<Directory "/var/www/html/wiki">
```

```
AuthBasicProvider ldap
```

```
AuthType Basic
```

```
AuthzLDAPAuthoritative off
```

```
AuthName "test server"
```

```
AuthLDAPURL
```

```
"ldap://ubiq-serv1.companyname.local:389/DC=companyname,DC=local?sAMAccountName?sub?(o
```

```
NONE
```

```
AuthLDAPBindDN
```

```
"CN=ldap45457,CN=Users,DC=companyname,DC=local"
```

```
AuthLDAPBindPassword *****
```

```
require valid-user
```

```
</Directory>
```

heres the error when I tried to login as me, note the bind failure.

```
[Mon Mar 24 12:32:38 2008] [notice] Apache/2.2.3 (Red Hat) configured ---  
resuming normal operations
```

```
[Mon Mar 24 12:32:41 2008] [warn] [client 192.168.117.1] [16839]  
auth_ldap authenticate: user marsh authentication failed; URI /wiki/index.php  
[LDAP: ldap_simple_bind_s() failed][Invalid credentials]
```

```
[Mon Mar 24 12:32:41 2008] [error] [client 192.168.117.1] user marsh:  
authentication failure for "/wiki/index.php": Password Mismatch
```

```
[Mon Mar 24 12:32:43 2008] [warn] [client 192.168.117.1] [16836]  
auth_ldap authenticate: user marsh authentication failed; URI /wiki/index.php  
[LDAP: ldap_simple_bind_s() failed][Invalid credentials]
```

Re: LDAP Authentication from Linux

[Mon Mar 24 12:32:43 2008] [error] [client 192.168.117.1] user marsh:  
authentication failure for "/wiki/index.php": Password Mismatch

Dana Epp [Security MVP] wrote:

You can start by looking in /var/log to see what the bind failure error is. On the apache side, it might be as easy as /var/log/apache/error.log.

Depending how you have LDAP set up, remember that the user you configure must have privileges to query AD. But before we try to tackle the permission problems, lets see what the error is. If you don't see it in the error.log, check /var/log/syslog and /var/log/messages. Paste what you see in reference to your LDAP query, and we can go from there.

Regards,  
Dana Epp [Microsoft Security MVP]

"Adrian Marsh (NNTP)"  
<adrian.marsh@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message  
[news:u8JguRXIIHA.3512@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:u8JguRXIIHA.3512@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi All,

I'm trying to implement a secure authentication from an apache2 server across to my SBS2003 server.

I've configured LDAP in apache, and if I bind using a Domain Admin account then all is well and I can login.

However, I don't really want to use a domain admin account for this. So I setup a new user account, and have tried using that but the bind fails. I'm guessing its a permissions issue, but am not sure where to start to look.

Second, am I using the right mechanism here? Isn't LDAP for directory lookups and Kerberos for authentication??

Adrian

Re: LDAP Authentication from Linux