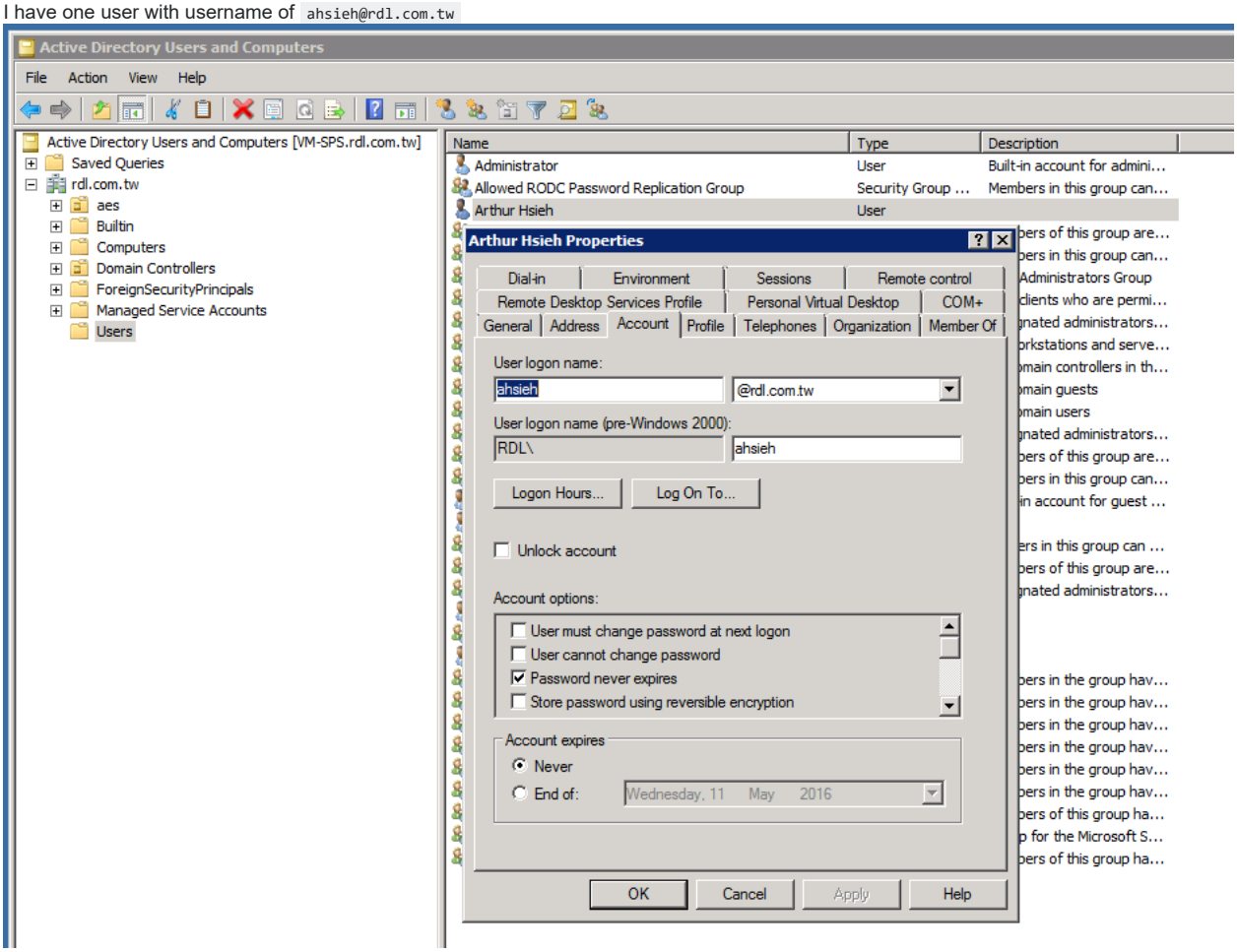
FailedLoginException encountered when using JAAS LdapLoginModule to authenticate with ActiveDirectory

I'm pulling my hair out try to get LDAP authentication to work with Active Directory.

We've just setup a SharePoint Server 2010 and we thought it would be a good idea to also authenticate users against the Active Directory given it's already there for SharePoint. Our environment is Windows Server 2008 R2 Standard.

I have one user with username of `ahsieh@rdl.com.tw`



According to this answer https://serverfault.com/a/130556 my provider URL should be `ldap://192.168.0.81:389/CN=Users,DC=rdl,DC=com,DC=tw` (note that instead of using the hostname of vm-sps.rdl.com.tw, I've elected to use the IP address as I've not had the time to configure DNS entry for the said server)

Just to be sure, I've run the dsquery command on the server:

```
C:\Users\Administrator>dsquery user -upn ahsieh@rdl.com.tw
"CN=Arthur Hsieh,CN=Users,DC=rdl,DC=com,DC=tw"

C:\Users\Administrator>
```

However, I just can't get the authentication work. I've tried all three type of JAAS config as per LdapLoginModule API

Below are the errors I encounter:

1. Search-first mode:

NOTE: I've NOT specified authzIdentity as I don't have that setup on AD

JAAS Config:

```
AESLogin_AD1 {
    com.sun.security.auth.module.LdapLoginModule REQUIRED
    userProvider="ldap://192.168.0.81:389/CN=Users,DC=rdl,DC=com,DC=tw"
    userFilter="(&(uid={USERNAME})(objectClass=User))"
    useSSL=false
    debug=true;
};
```

Result:

```
        [LdapLoginModule] search-first mode; SSL disabled
        [LdapLoginModule] user provider:
ldap://192.168.0.81:389/CN=Users,DC=rdl,DC=com,DC=tw
        [LdapLoginModule] searching for entry belonging to user: ahsieh@rdl.com.tw
        [LdapLoginModule] authentication failed
        [LdapLoginModule] aborted authentication
javax.security.auth.login.FailedLoginException: Cannot find user's LDAP entry
```

2. Authentication-first mode

JAAS Config:

```
AESLogin_AD2 {
    com.sun.security.auth.module.LdapLoginModule REQUIRED
    userProvider="ldap:///CN=Users,DC=rdl,DC=com,DC=tw"
    authIdentity="{USERNAME}"
    userFilter="(&(|(samAccountName={USERNAME})(userPrincipalName={USERNAME})(cn=
{USERNAME}))(objectClass=user))"
    useSSL=false
    debug=true;
};
```

Result:

```
        [LdapLoginModule] authentication-first mode; SSL disabled
        [LdapLoginModule] user provider: ldap:///CN=Users,DC=rdl,DC=com,DC=tw
        [LdapLoginModule] attempting to authenticate user: ahsieh@rdl.com.tw
        [LdapLoginModule] authentication failed
        [LdapLoginModule] aborted authentication
javax.security.auth.login.FailedLoginException: Cannot bind to LDAP server
```

3. Authentication-only mode

NOTE: I've NOT specified authzIdentity as I don't have that setup on AD

JAAS Config:

```
AESLogin_AD3 {
    com.sun.security.auth.module.LdapLoginModule REQUIRED
    userProvider="ldap://192.168.0.81:389"
    authIdentity="CN={USERNAME},CN=Users,DC=rdl,DC=com,DC=tw"
    useSSL=false
    debug=true;
};
```

Result:

```
        [LdapLoginModule] authentication-only mode; SSL disabled
        [LdapLoginModule] user provider: ldap://192.168.0.81:389
        [LdapLoginModule] attempting to authenticate user: ahsieh@rdl.com.tw
        [LdapLoginModule] authentication failed
        [LdapLoginModule] aborted authentication
javax.security.auth.login.FailedLoginException: Cannot bind to LDAP server
```

I've also tried another config based on some examples I've come across on the internet:

4. Config from other example

JAAS Config:

```
AESLogin_AD4 {
    com.sun.security.auth.module.LdapLoginModule REQUIRED
    userProvider="ldap://192.168.0.81:389/CN=Users,DC=rdl,DC=com,DC=tw"
    authIdentity="{USERNAME}"
    useSSL=false
    debug=true;
};
```

Result:

```
        [LdapLoginModule] authentication-only mode; SSL disabled
        [LdapLoginModule] user provider:
ldap://192.168.0.81:389/CN=Users,DC=rdl,DC=com,DC=tw
        [LdapLoginModule] attempting to authenticate user: ahsieh@rdl.com.tw
        [LdapLoginModule] cannot create LdapPrincipal: bad DN
        [LdapLoginModule] authentication failed
        [LdapLoginModule] aborted authentication
javax.security.auth.login.FailedLoginException: Cannot create LdapPrincipal
```

NOTE: My fourth trial seems to show slight progress, as at least LDAP binding seems to work but now the issues seems to be `cannot create LdapPrincipal: bad DN`

I've gone into the source code for `LdapLoginModule` and by matching the debug message, seems this was caused by (starting Line 837):

```
try {

    ldapPrincipal = new LdapPrincipal(dn);

} catch (InvalidNameException e) {
    if (debug) {
        System.out.println("\t\t[LdapLoginModule] " +
                           "cannot create LdapPrincipal: bad DN");
    }
    throw (LoginException)
        new FailedLoginException("Cannot create LdapPrincipal")
            .initCause(e);
}
```

And based on the LdapPrincipal API, `InvalidNameException` is thrown *If a syntax violation is detected*, but I have no idea where the syntax violation is.

Nor have I any idea how to debug this.

Any help will be much appreciated! Thanks!

java authentication active-directory ldap jaas

`LdapPrincipal` expects a distinguished name, which "ahsieh@rdl.com.tw" is not. In the last example, for instance (assuming the particular account is permitted to bind to the directory) try to set `authIdentity` to `CN={USERNAME},CN=Users,DC=rdl,DC=com,DC=tw` and log in as "ahsieh@rdl.com.tw"; or leave `authIdentity` as is and log in as `CN=ahsieh@rdl.com.tw,CN=Users,DC=rdl,DC=com,DC=tw` . – Uux Apr 13 '16 at 10:39

Thanks @Uux, unfortunately both of your suggestions results in `javax.security.auth.login.FailedLoginException: Cannot bind to LDAP server` Any other thoughts on what I can try? Thanks. – Arthur Apr 13 '16 at 15:36

My bad, I failed to notice that `userProvider` already contained a base DN there, hence its combination with my proposed `authIdentity` value obviously refers to a nonexistent entry (`CN=ahsieh@rdl.com.tw,CN=Users,DC=rdl,DC=com,DC=tw,CN=Users,DC=rdl,DC=com,DC=tw`). A further mistake in my suggestion was that `ahsieh@rdl.com.tw` is probably (I'm not familiar with Active Directory's schema(ta)) the `userPrincipalName` attribute, rather than the `CN` one. I won't further speculate about this though, since you've apparently figured it out yourself. – Uux Apr 13 '16 at 17:35

1 Answer

I've gone through many more articles on the net and finally found the solution from Bonitasoft's Q&A JAAS config for Active Directory LDAP

JAAS Config:

```
AESLogin_ADx {
    com.sun.security.auth.module.LdapLoginModule REQUIRED
    userProvider="ldap://192.168.0.81:389/CN=Users,DC=rdl,DC=com,DC=tw"
    authIdentity="{USERNAME}@rdl.com.tw"
    userFilter="(&(|(samAccountName={USERNAME})(userPrincipalName={USERNAME})(cn={USERNAME}))(objectClass=user))"
    useSSL=false
    debug=true;
};
```

Result:

```
[LdapLoginModule] authentication-first mode; SSL disabled
[LdapLoginModule] user provider: ldap://192.168.0.81:389/CN=Users,DC=rdl,DC=com,DC=tw
[LdapLoginModule] attempting to authenticate user: ahsieh
[LdapLoginModule] searching for entry belonging to user: ahsieh
[LdapLoginModule] found entry: CN=Arthur Hsieh,CN=Users,DC=rdl,DC=com,DC=tw
[LdapLoginModule] authentication succeeded
[LdapLoginModule] added LdapPrincipal "CN=Arthur Hsieh,CN=Users,DC=rdl,DC=com,DC=tw" to
Subject
[LdapLoginModule] added UserPrincipal "ahsieh" to Subject
```

answered Apr 13 '16 at 16:22

Arthur
170 ● 2 ● 12