

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg02242

- *From:* ohaya <ohaya@xxxxxxx>
 - *Date:* Sun, 28 Jan 2007 18:17:29 -0500
-

Joe,

Can you clarify what you meant by:

"if someone has set a specific UPN other than what you think it is (i.e. the domain default UPN)..."

How is the "domain default UPN" set?

Thanks,
Jim

Joe Richards [MVP] wrote:

If you have two objects with the same upn, that upn will be unuseable. Also if someone has set a specific UPN other than what you think it is (i.e. the domain default UPN) that has caused a tremendous number of issues that I have seen people running into. Also if you can't reach a GC (assuming multiple domains) using UPNs will fail as well. That shouldn't impact NT style userid though. I would recommend getting a trace of the requests and look at the extended error info unless your SDK allows you to dump that directly.

--

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

ohaya wrote:

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

Hi,

I was just fooling around with a few ideas about the original problem, and I did the following:

I originally had a user in AD, "cn=baduser,cn=users,dc=test,dc=com".

I created a OU, "foo-ou" at the same level as the "cn=users,dc=test,dc=com".

I used ldifde to import a new user:

```
dn: CN=baduser1,OU=foo-ou,DC=test,DC=com
changetype: add
cn: baduser1
displayName: test1
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=test,DC=com
objectClass: user
name: test1
sAMAccountName: baduser1
userPrincipalName: baduser@xxxxxxxx
```

This ldifde worked.

So now I have two users in AD:

```
dn: CN=bad user,CN=Users,DC=test,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: bad user
sn: user
givenName: bad
distinguishedName: CN=bad user,CN=Users,DC=test,DC=com
instanceType: 4
whenCreated: 20070126065002.0Z
whenChanged: 20070126065003.0Z
displayName: bad user
uSNCreated: 49165
uSNChanged: 49170
name: bad user
objectGUID:: HyipJ7V.....2D6rQ==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 128142691415621280
```

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

pwdLastSet: 128142678031804560
primaryGroupID: 513
objectSid:: AQUAAAAAAAA.....LGOezaxDWgQAAA==
accountExpires: 9223372036854775807
logonCount: 2
sAMAccountName: baduser
sAMAccountType: 805306368
userPrincipalName: baduser@xxxxxxx
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=test,DC=com

dn: CN=baduser1,OU=foo-ou,DC=test,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: baduser1
distinguishedName: CN=baduser1,OU=foo-ou,DC=test,DC=com
instanceType: 4
whenCreated: 20070126070303.0Z
whenChanged: 20070126070520.0Z
displayName: test1
uSNCreated: 49174
uSNChanged: 49177
name: baduser1
objectGUID:: m1GB8C.....tF77cQ==
userAccountControl: 546
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 128142687207770688
primaryGroupID: 513
objectSid:: AQUAAAAAAAAAU.....iFmLGOezaxDXAQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: baduser1
sAMAccountType: 805306368
userPrincipalName: baduser@xxxxxxx
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=test,DC=com

Note that the two users above have the same userPrincipalName, "baduser@xxxxxxx".

I'm wondering if, somehow (and I don't know how!), something like this could be what we have?

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

Question: *IF* somehow we ended up with two users as the above, with the same userPrincipalName, could that cause the symptoms that I'm seeing, where I can do the simple bind with full DN, but not with UPN?

BTW, using a simple bind with ldifde using:

```
cn=baduser1,ou=foo-ou,dc=test,dc=com  
OR  
test.com\baduser1
```

fails, i.e., I can't seem to bind with that 2nd user at all.

Jim

ohaya wrote:

Hi,

I went onsite again, and while there, did more investigating.

According to what I was told today, there is only the one AD ("tempad.foo.foo1") for the "foo.foo1" domain, and workstations are joined to the "foo" domain.

So, I'm kind of back to my earlier question: What would prevent simple LDAP binds with usernames in the UPN format or in the NT format fail, but full DN formatted usernames would work?

I don't know if this is related, but I checked the Event Viewer on the "tempad" machine, and found pairs of errors/warnings:

```
Error: Event Id: 4007  
Source: DNS  
Data: 0d 00 00 00
```

```
Warning: Event Id: 706
```

Jim

ohaya wrote:

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

Joe,

FYI, I've just sent off an email with my "analysis" of what may be going on in this one, particular environment. Basically, I'm theorizing that there are two factors at work here:

- 1) Having the two AD machines with exactly the same Windows domain name (but different hostnames, and different IP addresses), and
- 2) Some behavior which I/we haven't been able to identify with the way that AD handles simple LDAP binds, among the 3 different username formats.

I've suggested that they can either:

- 1) Leave things as-is, since my web app is now working, or
- 2) Re-configure things into a more "orthodox" configuration. In particular, I've suggested/recommended that they eliminate the "2nd AD", and let me point my web app at the "1st" ("real") AD/Domain controller, since this is how the other sites are configured.

I wasn't involved in the original decision to standup the "2nd AD", so I don't know exactly why they did that, but this particular site is suppose to be testbed-type site, so it's suppose to resemble the other sites as closely as possible anyway.

My guess is someone was overly risk-averse and didn't want to have the web app affecting the "1st AD" (strange, since this web app is already in production at 3 other sites :)!)..

I'd still be interested if anyone has any insight into what is going on with the current, admittedly strange, configuration, in particular as to how and why this would interact with the format of the usernames

Re: Possible scenario? was Re: HELP! Really strange problem w/AD and LDAP/LDIFDE

used for the simple LDAP binds!!

Thanks again!

Jim

Joe Kaplan wrote:

I think you may be on to something here, as there may be some additional involvement with DNS and/or the GC in order to service the simple bind with UPN username and perhaps that is behaving weirdly in this environment due to something in its "checkered" past. :)

However, I'm clueless on this level of detail, so I'd want someone from MS (or a more useful MVP type :) to step in and hopefully elaborate on what's going on under the hood.

Joe K.