

Re: DirectorySearcher – SearchResult – User Groups

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2004-12/0208.html>

From: Joe Kaplan \((MVP – ADSI)\) (*joseph.e.kaplan_at_removethis.accenture.com*)

Date: 12/16/04

Date: Thu, 16 Dec 2004 09:43:08 -0600

You probably want the DN for your search root to be the domain root, which is likely to be:

DC=corp,DC=isacorp,DC=com

The search below uses the actual user's DN (making the search not really necessary at all), so it would need to be base-level if you were going to do that.

That said, I don't recommend the approach suggested by that article for getting group membership. I think you should consider using tokenGroups instead to discover security group membership. If you do some Google groups searches on tokenGroups, you should see some samples.

Joe K.

"George Durzi" <gdurzi@hotmail.com> wrote in message
news:OVaffC44EHA.1596@tk2msftngp13.phx.gbl...

> Hi,

> I'm having trouble fetching the AD groups a user belongs to after

> authenticating them against Active Directory. My code is based on the How

> To for using Forms Authentication to authenticate against AD

> (<http://support.microsoft.com/default.aspx?scid=kb;en-us:326340>)

>

> LDAP ConnectString:

> LDAP://VN-SRV-DC01.corp.isacorp.com/DC=corp,DC=isacorp,DC=com

> Domain Name: VN-SRV-DC01.corp.isacorp.com

>

> Initially, when I use the DirectorySearcher to find cn=gdurzi, the path of

> the results is:

> LDAP://VN-SRV-DC01.corp.isacorp.com/CN=gdurzi,CN=Users,DC=corp,DC=isacorp,DC=com

>

> My code does the following to get the users groups does the following:

>

> DirectorySearcher oDS = new

>

```
DirectorySearcher("LDAP://VN-SRV-DC01.corp.isacorp.com/CN=gdurzi,CN=Users,DC=corp,DC=isacorp,DC=com")
> oDS.Filter = "(cn=gdurzi)";
> oDS.PropertiesToLoad.Add("memberOf");
> try {
> SearchResult oSR = oDS.FindOne();
>
> I get an Exception on the call to FindOne. "The specified domain either
> does not exist or could not be contacted"
>
> After binding to the VN-SRV-DC01.corp.isacorp.com domain in ldp.exe, I can
> do a search for cn=gdurzi successfully by using a Base DN of:
> CN=Users,DC=corp,DC=isacorp,DC=com
>
> ***Searching...
> ldap_search_s(ld, "CN=Users,DC=corp,DC=isacorp,DC=com", 1, "CN=gdurzi",
> attrList, 0, &msg)
> Result <0>: (null)
> Matched DNs:
> Getting 1 entries:
>>> Dn: CN=gdurzi,CN=Users,DC=corp,DC=isacorp,DC=com
> 4> objectClass: top; person; organizationalPerson; user;
> 1> cn: gdurzi;
> 1> distinguishedName: CN=gdurzi,CN=Users,DC=corp,DC=isacorp,DC=com;
> 1> name: gdurzi;
> 1> canonicalName: corp.isacorp.com/Users/gdurzi;
>
>
> If I open the enterprise tree in ldp.exe and find my cn, here's what I
> get:
>
> Expanding base 'CN=gdurzi,CN=Users,DC=corp,DC=isacorp,DC=com'...
> Result <0>: (null)
> Matched DNs:
> Getting 1 entries:
>>> Dn: CN=gdurzi,CN=Users,DC=corp,DC=isacorp,DC=com
> 4> objectClass: top; person; organizationalPerson; user;
> 1> cn: gdurzi;
> 1> sn: Durzi;
> 1> givenName: George;
> 1> distinguishedName: CN=gdurzi,CN=Users,DC=corp,DC=isacorp,DC=com;
> 1> instanceType: 4;
> 1> whenCreated: 11/24/2004 22:38:51 US Mountain Standard Time US Mountain
> Standard Time;
> 1> whenChanged: 12/16/2004 7:58:12 US Mountain Standard Time US Mountain
> Standard Time;
> 1> displayName: George Durzi;
> 1> uSNCreated: 8471;
> 2> memberOf: CN=FrameworkAdmins,CN=Users,DC=corp,DC=isacorp,DC=com;
> CN=Remote Desktop Users,CN=Builtin,DC=corp,DC=isacorp,DC=com;
> 1> uSNChanged: 349743;
> 1> name: gdurzi;
```

> 1> objectGUID: 2975a92e-fb4b-4141-a0de-482dca83d95b;
> 1> userAccountControl: 0x10200;
> 1> badPwdCount: 0;
> 1> codePage: 0;
> 1> countryCode: 0;
> 1> badPasswordTime: <ldap error <0x0>: cannot format time field;
> 1> lastLogon: <ldap error <0x0>: cannot format time field;
> 1> logonHours: <ldap: Binary blob>;
> 1> pwdLastSet: <ldap error <0x0>: cannot format time field;
> 1> primaryGroupID: 513;
> 1> userParameters: m: d ;
> 1> objectSid: S-1-5-21-1561616353-131408304-1539857752-1612;
> 1> accountExpires: 0;
> 1> logonCount: 12;
> 1> sAMAccountName: gdurzi;
> 1> sAMAccountType: 805306368;
> 1> userPrincipalName: gdurzi;
> 1> objectCategory:
> CN=Person,CN=Schema,CN=Configuration,DC=corp,DC=isacorp,DC=com;
> 1> msNPAllowDialin: TRUE;
> -----
>
> You can see that the memberOf property properly pulls the groups my cn is
> a member of:
>
> memberOf: CN=FrameworkAdmins,CN=Users,DC=corp,DC=isacorp,DC=com; CN=Remote
> Desktop Users,CN=Builtin,DC=corp,DC=isacorp,DC=com;
>
>
> Any idea why my code is error'ing at the call to FindOne?
>