

RE: validaing security using AD groups... in web.config

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2007-11/msg00525.html>

- *From:* stcheng@xxxxxxxxxxxxxxxxxxxxxx (Steven Cheng[MSFT])
 - *Date:* Tue, 06 Nov 2007 09:30:00 GMT
-

Hi Nalaka,

From your description, you're using ASP.NET membership provider and want to use AD groups (roles) for authorization in the application ,correct?

Based on the web.config segment you provided, you configured the following things:

```
** set membership service to use ADMembershipprovider
** add authorization setting to allow only members of
"bctgtwdom\someADSecurityGroup" AD group to visit default.aspx
```

However, the problem is that if you use "roles" rather than "users" in <authorization> entry, that means you use the current user's roles to perform authorization check. So only configuring membership provider is not enough. Membership provider only help authenticate the user(verify the user through the given username/password credentials).

Therefore, for the case here, what you need is a RoleManager provider which can query the AD windows roles of a given user:

#How To: Use Role Manager in ASP.NET 2.0
http://msdn2.microsoft.com/en-us/library/ms998314.aspx#paght000013_step4

There is a built-in windowsTokenRoleProvider in ASP.NET 2.0:

```
#WindowsTokenRoleProvider Class
http://msdn2.microsoft.com/en-us/library/system.web.security.windowstokenroleprovider.aspx
```

Or you can implement your own AD Role provider through ADSI codes since the built-in one may have some limitation and not quite flexible.

```
#WindowsTokenRoleProvider - Dominick's view
http://www.pluralsight.com/blogs/keith/archive/2006/05/31/26192.aspx
```

RE: validaing security using AD groups... in web.config

Sincerely,

Steven Cheng

Microsoft MSDN Online Support Lead

=====

Get notification to my posts through email? Please refer to <http://msdn.microsoft.com/subscriptions/managednewsgroups/default.aspx#notifications>.

Note: The MSDN Managed Newsgroup support offering is for non-urgent issues where an initial response from the community or a Microsoft Support Engineer within 1 business day is acceptable. Please note that each follow up response may take approximately 2 business days as the support professional working with you may need further investigation to reach the most efficient resolution. The offering is not appropriate for situations that require urgent, real-time or phone-based interactions or complex project analysis and dump analysis issues. Issues of this nature are best handled working with a dedicated Microsoft Support Engineer by contacting Microsoft Customer Support Services (CSS) at <http://msdn.microsoft.com/subscriptions/support/default.aspx>.

=====

This posting is provided "AS IS" with no warranties, and confers no rights.

From: "Nalaka" <nalaka12@xxxxxxxxxxxxxx>
Subject: validaing security using AD groups... in web.config
Date: Mon, 5 Nov 2007 17:14:09 -0800

Hi,
I am testing with an asp.net 2.0 app.... has only one page Default.aspx.
I want to deny all users except for a certain AD group.
I did the following... but app keeps allowing everyone in.
What am I doing wrong?

```
<configuration>  
<connectionStrings>  
<add name="ADConnectionString"  
connectionString="LDAP://gtwds7eap01 />
```

RE: validaing security using AD groups... in web.config

RE: validaing security using AD groups... in web.config

</connectionStrings>

<system.web>

<identity impersonate="true"/>

<authentication mode="Windows"/>

<membership defaultProvider="MembershipADProvider">

<providers>

<add name="MembershipADProvider"

type="System.Web.Security.ActiveDirectoryMembershipProvider"

connectionStringName="ADConnectionString"

connectionUsername=""

connectionPassword=""/>

</providers>

</membership>

</system.web>

<location path="Default.aspx">

<system.web>

<authorization>

<allow roles=" bctgtwdom\someADSecurityGroup"/>

<deny users="*/>

</authorization>

</system.web>

</location>

</configuration>

Any help is deeply appreciated

Thanks

Nalaka