

Re: ASP using ADSI

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-04/msg00135

- *From:* JT <JT@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 4 Apr 2006 06:42:02 -0700
-

Joe,

First of all, let me just say that I am not a programmer by any stretch of the imagination. I'm using ASP because I know nothing of .net. When I started this project, I went out looking for scripts that could do what I needed done, and started using vbscript. I then decided a web interface of sorts would be good, since most of the people that will be using it are not very computer savvy (trying to be nice...). As for the posting, I wasn't sure what group would be the best to assist in my problem, so thanks for taking the time...:)

My environment is an NT4 domain that is being migrated to W2K3 AD domain. The users reside in the NT4 domain and will continue to do so until all the systems are migrated. The groups and the web server, however, are located in the W2K3 AD domain. I created a group in the W2K3 AD domain that had delegation to add/remove users in groups. The web server has delegation for kerberos and uses windows authentication, and IE on the client machine has windows auth enabled. When I originally created the ASP page, I was able to get everything working as long as the users, groups, and web server were in the W2K3 AD domain. I would bind to everything using LDAP, and the authenticated user would be able to do his/her thing.

The problems all began when trying to do the same thing with users being in NT4 domain. Binding seemed to be an issue, so that is why I went to the WinNT standard. Now the issues revolve around authentication. From the web server, everything works great. From the client machine I can run vbscripts directly against AD and they work, but connecting to the ASP and allowing the server to perform the operation fails. I've tried many variations of the GetObject without success. Needless to say, I'm about to pull what little hair I have left out of my head...:) I decided to try a service account so authentication would be done against that account and not an NT4 domain account – still no luck. I thought about trying to convert the NT4 credentials to DN's. I hope some of this makes sense.

Joel

"Joe Kaplan (MVP – ADSI)" wrote:

Re: ASP using ADSI

A couple of things:

- Coding questions using go in the microsoft.public.adsi.general newsgroup :)
- Why on earth would you use WinNT to manage an AD domain? LDAP is the preferred method.
- I'm a .NET guy, so I usually don't answer the ASP questions. I think ASP sucks big time and never want to program in it again. :) However, I will try to help.
- When you say you set up a service account, exactly how are those credentials being used here? ASP will automatically impersonate the logged in user, so depending on your security settings in IIS, that will either be the authenticated user or the anonymous user.

Joe K.

"JT" <JT@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:37C32E1A-A9AB-4BBA-9E80-A918C7F625F6@xxxxxxxxxxxxxxxxxxxx

Joe,

The ASP page is basically an access control page being created to give some group managers and our help desk the ability to add and remove users from groups with access to certain files and folders. I created a group with the delegation of control to add and remove users from groups in an OU, and placed these individuals in the group. I've created the service account, but it is still failing. It is giving different errors depending on how I bind to the objects. Here are some things I've tried so far:

```
set objDomain = GetObject("WinNT://2003 AD Domain")
set objGroup = objDomain.GetObject("Group", strGroupDN)
objGroup.Add("WinNT://NT4 Domain/" & strMemberDN)

set objUser = GetObject("WinNT://NT4 Domain/" & strMemberDN)
set objGroup = GetObject("WinNT://2003 AD Domain/" & strGroupDN)
objGroup.Add(objUser.ADsPath)
```

The errors seem to be related to either not finding the path or access being denied.

Any thoughts?

Joel

"Joe Kaplan (MVP - ADSI)" wrote:

Re: ASP using ADSI

If you can use a service account in your app to do what you need to do, then that should work fine. This really just depends on what you need to do in your AD query and whether it requires the authenticated user's credentials or not.

Kerberos delegation requires the ability to authenticate a user with Kerberos in the first place, so that isn't going to fly with NT4 users. I'm glad you are migrating. :)

Joe K.

"JT" <JT@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:14FA4117-9876-44E2-B558-35ABCDC3FB0E@xxxxxxxxxxxxxxxxxxxx

Hey Joe,

Thanks for the reply. I think the problem is occurring because of how the domain is configured at the moment. We are in the process of migrating from NT4 domain to 2003. The users are still in the NT4 domain, and the groups are in 2003 AD. If I use an account on the remote system within the AD domain, the page works. If I log on using an NT domain account, it gives me the error. I'm trying to figure out the best way around this. I want to use authentication to the page so not just anyone can access it. I'm thinking about creating a service account in the 2003

Re: ASP using ADSI

that will be used to query
AD.
Any thoughts/suggestions on this?

Thanks,
Joel