

## Re: ADAM bindable object question

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2004-03/1148.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-03/1148.html)

---

**From:** Bob Durie (*bobdurie\_at\_canada.com*)

**Date:** 03/18/04

Date: 18 Mar 2004 15:21:34 -0800

Thanks for the reply, that actually makes a lot of sense. I guess I can do that with ldif scripts, using the systemAuxiliaryClass attribute – i don't think i can change this attribute value at creation time with the ADAM schema snapin... please correct if I'm wrong.

As for the non-conformant schema, LDAP modify operations with multiple attribute changes would typically solve this problem. That's what I'm trying to do, and have done in the past when an auxiliary object class has mandatory attributes for other directory products... sample ldif below:

```
dn: OU=wannabind,O=corp,C=ca
changetype: modify
add: objectClass
objectClass: msDS-bindProxy
add: objectSid
objectSid:: AQUAAWAAAAUVAAAAaHCdCs9LDWSdu0M89AEAAA==
```

But obviously this doesn't work. I was very happy to hear AD for w2k3 (and ADAM) allowed for dynamically adding object classes to entries – it would be nice if the above worked too, but oh well (maybe for the next AD :).

One more followup question – is there any way (for instance, using the userPassword or unicodePwd attributes) to make an existing object bindable if it's structural objectclass doesn't allow for it (either through optional attributes, or static auxiliary classes as you've described)? Basically, for an existing entry of \*arbitrary\* object class, can it's DN be used to authenticate to the directory? This would typically be done in X.500 by adding the 'simpleAuthObject' auxiliary object class to the entry, and then assignment of the userPassword attribute... it seems for ADAM the answer is no, but I just want to be sure.

Thanks!  
Bob

"Dmitri Gavrilov [MSFT]" <dmitrig@online.microsoft.com> wrote in message news:<#aIR2OSDEHA.712@tk2msftngp13.phx.gbl>...

> You can not add msDS-bindableObject or msDS-bindProxy to an existing object.  
> You have to add them to a class definition in the schema, which will make  
> all objects of this class behave the same way. Moreover, you must add them  
> at the time when you create your class -- you will not be able to update it  
> later on. This is because adding the aux class adds a new mustContain  
> (objectSid), and this is not allowed for existing classes. The reason for  
> not allowing this is you could have existing objects of this class, and this  
> addition would make them invalid (non schema-conformant).

>  
> Bottom line -- include msDS-bindableObject or msDS-bindProxy aux class to  
> your class definition, at creation time.

>  
> --

> Dmitri Gavrilov  
> SDE, Active Directory Core

>  
> This posting is provided "AS IS" with no warranties, and confers no rights.  
> Use of included script samples are subject to the terms specified at  
> <http://www.microsoft.com/info/copyright.htm>

>  
> "Bob Durie" <bobdurie@canada.com> wrote in message  
> news:b4ec8b59.0403181030.df9e439@posting.google.com...

> > Hi there,  
> >

> > I'm having difficulty create security principals (or proxies) out of  
> > arbitrary entries in ADAM. My goal is to have a plain old entry  
> > (non-user), add either the msDS-bindableObject or msDS-bindProxy  
> > objectClass, and allow that entry to authenticate. I've read some  
> > similar posts on here about this, but no one has my specific problem.

> >  
> > The problem I'm seeing is when i try to add these object classes  
> > (using either ldifde or ldap), i have issues with the objectSid  
> > attribute. In the case of adding msDS-bindableObject to an entry,  
> > objectSid is a required attribute and I don't know how to construct  
> > one! Hence, i get the "A required attribute is missing" error. When  
> > I try to add msDS-bindProxy and use an existing SID from a real AD (or  
> > ADAM) user, I get this:

> >  
> > Add error on line 1: Unwilling To Perform  
> > The server side error is: 0x20e7 The modification was not permitted  
> > for security  
> > reasons.

> > The extended server error is:  
> > 000020E7: SvcErr: DSID-03152972, problem 5003 (WILL\_NOT\_PERFORM), data  
> > 8358

> >  
> > I've seen posts that allude to the possibility you cannot dynamically  
> > extend an existing entry with these objectclass's, it must be a  
> > statically linked auxiliary class -- but when i try to make a

microsoft.public.windows.server.active\_directory: Re: ADAM bindable object question

> > *structural object class have a static auxiliary linking to on of the*  
> > *msDS-bind\* object classes I get "The change was rejected by the*  
> > *directory service." error. Help!! I know there's some MS folk out*  
> > *there that have just the answer's i'm looking for, thanks!*  
> >  
> > *Bob Durie*