

# Re: AD Schema Extension Question

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-11/msg01213](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-11/msg01213)

---

- *From:* Oliver <[Oliver@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Oliver@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 22 Nov 2007 13:52:00 -0800
- 

Thanks Joe – i thought as much.

As far as information regarding recommendations on schema extensions goes, do you know of any white papers or tech articles that go into the detail you have mentioned?

i did find this:

<http://blogs.msdn.com/alextech/archive/2007/05/16/active-directory-schema-design-considerations-and-auxiliary-cl>

and of course the various MS articles...

and they are OK...but are more from the 'AD as a whole' rather than on the data contained in the extension (class/attrib) itself.

You know, you could write one? On top of everything else you are already doing.. ;)

Thanks again for your help – now when someone asks me 'i want to extend the schema!' i can make much more informed suggestions and give better advice (hopefully).

"Joe Kaplan" wrote:

The rangeUpper recommendation is mostly there as a safeguard to help protect the directory. If you make it as small as you can get away with that still allows the amount of data you actually plan to store, you help prevent someone from accidentally or maliciously using their permissions to put more data in your directory than you want or can handle. It is just a safety valve.

Joe K.

--

Joe Kaplan–MS MVP Directory Services Programming  
Co–author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>

--

Re: AD Schema Extension Question

"Oliver" <Oliver@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
news:6E595C08-B491-483A-9C6C-99B76B5F6129@xxxxxxxxxxxxxxxxxxxx

Mmm...sounds like (ADAM/sync) a bit of work there, and introduces another layer of complexity. Might just stick with the modification of the AD schema.

The rangeUpper values you mention are they implemented simply for protection and as a safeguard against directory bloat given that the app might get ambitious and mess up the dir. with excessive amounts of data? Or is there some other reasoning behind that..?

Anyway – your help has been invaluable, and has certainly spiked my interest in AD from a more programmatic POV... :)

thanks again!

"Joe Kaplan" wrote:

It could. You would need to have a user object in ADAM for each user in AD so there would be a place to actually put this attribute data which would imply that you would set up some sort of ongoing sync mechanism. If for whatever reason your eally didn't want this data in your main AD, that would be a reasonable way to solve that problem. The ADAM instances could be deployed much more narrowly so that they could support only the applications that need this data.

On the other hand, if you envision having lots of applications that need access to the same data and those apps might be deployed all over the place (but in the same locations that you have AD now), then AD might make a better choice.

My instinct on this type of thing is that if the data is for more than one

Re: AD Schema Extension Question

application and isn't going to make an impact on DIT size or replication that is a major concern, I'd just put it in AD. Going through the trouble to set up ADAM, get sync working and get ADAM deployed and replicating might not be worth it. Your own requirements will help you balance these two approaches and hopefully indicate which way is preferable. Other people tend to like to avoid putting this stuff in AD and will go for the ADAM approach first, so some of this is just disposition as to whether you like to extend the AD schema or not. :)

You could also put the data in SQL if you wanted to (or another LDAP directory). It all depends on what you need.

--  
Joe Kaplan--MS MVP Directory Services Programming  
Co--author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>  
--

"Oliver" <Oliver@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:ADE39366-1CD4-45B8-878D-B87F0C579543@xxxxxxxxxxxxxxxxxxxx](mailto:news:ADE39366-1CD4-45B8-878D-B87F0C579543@xxxxxxxxxxxxxxxxxxxx)

Thanks very much for the response Joe -- just the kind of suggestions i was looking for.

One other question though: could ADAM be used in a scenario such as this?

Thanks again. :)

"Joe Kaplan" wrote:

From a pure schema perspective, this is a pretty standard thing to do.

Re: AD Schema Extension Question

Make  
sure that an appropriate  
syntax for the datatype is  
being used  
(probably  
either octet string if storing  
data as binary or unicode  
string is  
storing  
as an encoded string). Also,  
make sure that rangeUpper  
is set  
appropriately  
to allow for the largest  
possible blob of data but  
doesn't allow  
unbounded  
data to be inserted. I also  
recommend setting  
schemaIDGUID on the  
attributes being added so  
that they will be the same in  
every  
directory  
they  
are imported into.

Unless you are doing linked  
attributes, there isn't a whole  
lot else  
to  
get  
wrong.

Joe K.

--

Joe Kaplan-MS MVP  
Directory Services  
Programming  
Co-author of "The .NET  
Developer's Guide to  
Directory Services  
Programming"  
<http://www.directoryprogramming.net>

--

"Oliver"  
<Oliver@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in message  
<news:13B507CF-B17C-4E7F-B6ED-4320A8023BE2@xxxxxxxxxxxxxxxxxxxx>

## Re: AD Schema Extension Question

have a customer that wants to extend the schema to include an attribute for an auxiliary class attached to the user class. The attribute will be used to store compressed and encrypted XML code with logon..and is currently used to store connection details for two applications – (its for an inhouse SSO app). They have registered the OID etc..Just wondering if there was anything to consider here? I was thinking DIT size/storage, replication

Re: AD Schema Extension Question

etc...but  
is  
there  
anything on  
the actual  
schema-side  
that may  
casue issues  
in  
the  
long  
term? I did  
refer to  
some AD  
books for  
some  
guidance..and  
googled  
but  
nothing  
(other than  
whats  
already  
mentioned  
here) really  
stood out.

rgds

O.