

Re: Export schema

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-12/1335.html

From: Dmitri Gavrilov [MSFT] (dmitrig_at_online.microsoft.com)

Date: 12/17/04

Date: Fri, 17 Dec 2004 10:43:02 -0700

Danny,

Forget defaultSDs, they are not the best solution. Put an inheritable ACE somewhere at the top of hierarchy and let it propagate down. You can even do this with the UI. It will be automatically stamped on all existing objects, and on any newly created ones (unless they are protected from inheritance).

It does not make sense to set defaultSD on aux classes, they will never apply.

If you need to make an attribute-specific ACE, you have to put schemaIDGUID off the attribute into the objectType field in the ACE.

WRT protecting an attribute from being read by everyone, it is difficult. In w2k3 sp1 we have a new attribute flag "CONFIDENTIAL", which will allow you to protect attributes from reading by everyone (even in the presence of default ACLs as they are today).

--

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>

"Danny Cooper" <danny.cooper@bbc.co.uk> wrote in message

news:pmh5s09hdbmapvmbk6etiod72991bc00um@4ax.com...

>

> I had been reading those links, plus many more, it just isn't clear

> enough for me to get a working solution.

>

> I get that the security on attributes is actually defined as a mask at

> the class level, and that you can specify either individual attributes

> or used a shared GUID for an attribute set.

>

> My problem is that in trying to interpret the tables, I cannot get a

> result that is useful.

>

> I am not trying to implement a security system via default security,

> just remove Authenticated Users from a specific set of new attributes,

> and grant SELF in its place.

>

> Things I think I've found:

Re: Export schema

microsoft.public.windows.server.active_directory: Re: Export schema

```
>  
> 1. security set on classes that are part of structural classes have  
> their security overruled by the structural class. I thought it would  
> "append" but it doesn't seem to  
>  
> 2. You can't "add to" a defaultSecurityDescriptor, you have to replace  
> it with one that includes new settings  
>  
> 3. It is so far impossible to stop Authenticated Users getting put  
> back in with Read All Properties - for no reason I can see  
>  
> 4. Setting the "P" flag in D:P(...) does turn off security inheritance  
> according to the schema MMC snap-in, but if a structural class that  
> includes your new aux class has it on by default, then instantiated  
> objects inherit too (overriding the aux class
```