

Re: Auditing changes in AD objects?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg00997

- *From:* Tomasz Onyszko <T.Onyszko_nospam_@xxxxxx>
 - *Date:* Thu, 14 Sep 2006 22:08:12 +0200
-

Jerry Mickman wrote:

Hi All,

I'm not new to directory services, but I'm from the Novell world, and I've only been working with AD in depth for a few months.

<matrix mode on>
Welcome to the real world
</matrix mode off>

(...)

So, we need to find out who's been changing the attributes on the objects.

You have to implement DS objects access auditing. You have to do two things:

1. Enable directory object access auditing

<http://technet2.microsoft.com/WindowsServer/en/Library/20068d03-6473-4e00-84d4-fb1c7cce57d21033.mspx>

2. Set SACLS on appropriate OUs, objects etc for groups or individuals which DS access You want to track

more about SACLS:

<http://technet2.microsoft.com/WindowsServer/en/Library/2f98f5b2-5e7e-4ff3-83a9-c32cf23329211033.mspx>

Novell's eDirectory has two attributes on their objects, creatorsname and modifiersname which records who created the object, and who last modified the object.

Do AD objects have similar attributes, and if so, how can I access them, since DSGET doesn't seem to be able to report their values.

AFAIK AD object has only whenCreated and whenChanged attributes

Re: Auditing changes in AD objects?

I'm thinking that what I need to do is run a complete audit on AD, going container by container, and seeing who has rights where. Any helpful hints on how to go about this? Again, I know how I'd do this from within eDirectory, but any helpful hints for AD would be very much appreciated. For instance, it doesn't look like you can use DSGET to report a list of AD trustee assignments for an OU, which would be very helpful.

but You can use dscls.exe:

<http://support.microsoft.com/kb/281146/>

or scripts.

--

Tomasz Onyszko

<http://www.w2k.pl/> - (PL)

<http://blogs.dirteam.com/blogs/tomek/> - (EN)

.