

## Re: Grant Object Access

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-08/0221.html>

---

**From:** Roger Abell (*mvpNOSpam\_at\_asu.edu*)

**Date:** 08/22/05

Date: Mon, 22 Aug 2005 08:14:01 -0700

Tweaking the ACL on the service will let the account inquire from the service control manager of the status of the server (or if granted start/stop/pause it).

What account can define a new scheduled task is under the internal control of the specific service code. I remember one time looking for how to adjust that, and not finishing the search. The blob at HKLM\Services\Schedule\Security is not what you are after (it is the launch/access info for the service, per the use of templates). It is probably the ACL on the "tasks" special folder, but I am not certain although there seems no security stored in the HKLM\Software\Microsoft\SchedulingAgent key. You probably need to try researching this, and then if needed posting a thread that makes clear your issue in its subject.

--

Roger Abell

Microsoft MVP (Windows Security)

MCSE (W2k3,W2k,Nt4) MCDBA

"Andrew Hayes" <AndrewHayes@discussions.microsoft.com> wrote in message news:%23KnD5AvpFHA.1996@TK2MSFTNGP10.phx.gbl...

> Yes. This is going to be used for anonymous web access, but since the user  
> has no control over the scheduled tasks in themselves (all the user can do  
> is upload a data file), I don't think there is much risk. When the upload  
is

> complete, the server automatically writes information about the datafile  
to

> a database, enumerates the tasks to see if the virus-scan is already  
> running, and if not then it creates a new task for starting a scan against  
> the file the user uploaded.

>

> As it happens, there was a mistake in the ASP code in that it wasn't  
setting

> one of our COM+ objects properties correctly, which was causing the follow  
> on exception, but I hadn't been able to see that until I had got it pass  
the

> Enumerating Scheduled Tasks error.

>

> As of this moment it all works correctly, so long as the IUSR\_ account is  
> part of the administrators group. Of course, that will not do in a  
> production environment.

>

> I'll go through the KB article you posted Roger and see if I can get it to  
> work that way. Last ditch attempt would be to use NTRights and add each  
> right until it succeeds in creating the task, then remove them all and try

## microsoft.public.windows.server.security: Re: Grant Object Access

> again until I can get the minimum needed for it to work.  
>  
> The other way would be for the ASP page to create the COM+ object under a  
> different identify, but I'm not sure how that works... More research is  
> needed.  
>  
> Regards...Andrew  
>  
> "Roger Abell" <mvpNOSpam@asu.edu> wrote in message  
> news:ulAwGitpFHA.3568@TK2MSFTNGP10.phx.gbl...  
> > The accesses you were being denied were to start and to query the  
> > service. I am not so sure that granting those will allow you to then  
> > schedule a new task, which your subsequent posts make it sound like  
> > you are trying to do. The way I adjust rights to services is to define  
> > a security config editor template that is new, hence totally empty,  
> > and then use the services node to edit the values for the concerned  
> > service, after which one uses the templated to analyze and configure  
> > the machine.  
> > That said, I have to wonder what in the world you are wanting to  
> > do this for . . . As it now appears, you are wanting to allow the  
> > Iusr\_ account to define new scheduled tasks, and/or to manage  
> > scheduled tasks. But the Iusr\_ account is not used for authenticated  
> > web access, so this means you are wanting to allow anonymous web  
> > browsers to tweek around in the machine's scheduled tasks ??? !!! #  
> > A recipe for disaster that sounds to be.  
> >  
> > --  
> > Roger Abell  
> > Microsoft MVP (Windows Security)  
> > MCSE (W2k3,W2k,Nt4) MCDBA  
> > "Andrew Hayes" <AndrewHayes@discussions.microsoft.com> wrote in message  
> > news:OFckn9spFHA.3084@TK2MSFTNGP09.phx.gbl...  
> >> False alarm. Sorry folks. :-(  
> >>  
> >> The reason I got past the previous error when trying to get service  
> >> status  
> >> was that I had added IUSR\_ to the local administrators group. Adding  
> the  
> >> Legacy Component does not correct the problem if I remove IUSR\_ from  
> the  
> >> local admin group.  
> >>  
> >> So the question is, what rights do I give IUSR\_ to allow it to use the  
> >> Schedule service correctly without making it a local administrator?  
> >>  
> >> I'll be taking a look at NTRights that Roger mentioned.  
> >>  
> >> Regards...Andrew  
> >>  
> >> "Andrew Hayes" <AndrewHayes@discussions.microsoft.com> wrote in message  
> >> news:uvhwk1spFHA.764@TK2MSFTNGP14.phx.gbl...  
> >> > From what you have said, Roger, and from what the various KB articles  
> >> > concerning that error has lead me to, is that the IUSER\_ account  
> >> > doesn't  
> >> > have the privileges. Right enough.  
> >> >  
> >> > Now, how to set those privileges?  
> >> >  
> >> > I finally found one way to do it.  
> >> >  
> >> > Using DCOMCNFG, I opened the COM+ library application that contains  
> all

## microsoft.public.windows.server.security: Re: Grant Object Access

```
> >> > the COM+ components for the web application, and tried adding a
> >> > "Component", selecting the Install New Component option and browsing
to
> >> > the MSTASK.DLL file. This gives me the error "One or more files do
not
> >> > contain component or type libraries. These files cannot be
installed."
> >> >
> >> > So much for Scheduler being a COM component, but then, I use COM to
> >> > work
> >> > with it from the VC++ code. Very strange. So I tried to add a new
> >> > "Legacy
> >> > Component"...
> >> >
> >> > Although the Scheduler doesn't show up with a human-friendly name, as
> >> > it
> >> > has no ProgID, it's CLSID was listed so I added it using that. Seemed
> >> > to
> >> > work, although it creates an icon with no name. I then changed the
> >> > identify of the created object to one that has local administrator
> > rights,
> >> > and gave local Launch, Activation and Access permissions to the local
> >> > IUSER_ and NETWORK_SERVICE accounts.
> >> >
> >> > Ran through my process again, and I no longer get the 560 for the
> > Schedule
> >> > object access but it is generating an Exception that I need to track
> >> > down.
> >> >
> >> > Still, I'm a little further along than I had been, and I hope what I
> >> > discovered would be useful to someone.
> >> >
> >> > Regards...Andrew
> >> >
> >> > "Roger Abell" <mvpNOSpam@asu.edu> wrote in message
> >> > news:utWtGYWpFHA.3940@TK2MSFTNGP14.phx.gbl...
> >> >>I am not aware what your COM+ component is attempting to do,
> >> >> but from the event message you post it would appear to me that
> >> >> a chain of events leading to attempt to get a handle to the Schedule
> >> >> service that allows querying and starting that service is denied.
> >> >> One does not grant rights to services in the ways you have attempted
> >> >> by altering the NTFS permissions on the binaries. Rather you need
> >> >> to either use security templates of such as NTrights.exe from the
> >> >> resource kit.
> >> >>
> >> >> --
> >> >> Roger Abell
> >> >> Microsoft MVP (Windows Security)
> >> >> MCSE (W2k3,W2k,Nt4) MCDBA
> >> >> "Andrew Hayes" <AndrewHayes@discussions.microsoft.com> wrote in
> >> >> message
> >> >> news:%23Xp7hLJpFHA.708@TK2MSFTNGP09.phx.gbl...
> >> >>> Hi All,
> >> >>>
> >> >>> As part of my continuing efforts to get COM+ components running
under
> >> >>> Windows 2003 Server SP1, I enabled Object Access auditing and File
> >> >>> auditing,
> >> >>> and ran through the process that is failing.
> >> >>>
> >> >>> One failure event was logged in the security log:
> >> >>>
```



microsoft.public.windows.server.security: Re: Grant Object Access

> >  
>  
>