

Re: system user

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2005-04/msg00856.html>

- *From:* "zengfeng" <zengfeng@xxxxxxxx>
 - *Date:* Mon, 18 Apr 2005 10:00:29 +0800
-

Thanks ,y r right! I have got it!

"Ray Trent" <ratrent@xxxxxxxx>

?????:eqSpJReQFHA.2132@xxxxxxxxxxxxxxxxxxxxxxxx

> Look for "Client impersonation" in the SDK documentation. The API you
> want is probably ImpersonateLoggedOnUser, though it might be a bit
> trickier if you're trying to do this from a kernel mode driver.

>

> zengfeng wrote:

>> "have the LOCAL SYSTEM process impersonate that user ",this is my
need.But

>> I don't know how to do ,can y tell me?

>> "Ray Trent" <ratrent@xxxxxxxx>

>> ?????: #kWFsuQFHA.3704@xxxxxxxxxxxxxxxxxxxxxxxx

>>

>>>The SYSTEM account has unlimited privileges (typically) on the local
>>>machine, but it has no credentials at all on some other host out there
>>>in the world, as far as I know. Hence it is usually referred to as the
>>>LOCAL SYSTEM account (though now that I look I don't see anything like
>>>that in the user namespace... instead it seems to be SYSTEM).

>>>

>>>Theoretically you might be able to grant access to "<hostname>\\SYSTEM"
>>>on the files that you want to access on the network, but a better
>>>solution (especially in a domain) would be to have an actual user
>>>account, very much preferably that of the user that is actually logged
>>>in, and grant that account access. Then have the LOCAL SYSTEM process
>>>impersonate that user when trying to access the file.

>>>

>>>I'm guessing that the reasoning for not letting SYSTEM have access to
>>>remote files is a security one. Since the SYSTEM account is the same no
>>>matter what user is logged on (or what process is trying to gain
>>>access), there's no way to track accesses to the file.

>>>

>>>>I want to use ZwCreateFile to open a network file in the system
>>>process.but

>>>>It 's always failed.I think it's caused by the privileges of system

>>>

>>> user.

>>>

Re: system user

> >>"Ray Trent" <ratrent@xxxxxxxxxxxx>
> >>?????:#xcTwNFQFHA.3076@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
> >>
> >>>Yes, that's typically the LOCAL SYSTEM account. And no, you can't
modify
> >>>it's privileges significantly without screwing up the whole OS.
> >>>
> >>>Once again, though: What are you *really* trying to accomplish by this?
> >>>There is no reason I can think of to want to do what you're asking...
> >>>
> >>>zengfeng wrote:
> >>>
> >>>>When y open the task manager,y will see some thread which create by
> >>
> >>system
> >>
> >>>>user. I think It's created by OS.
> >>>>"Pavel A." <pavel_a@xxxxxxxxxxxxxxxx> Ð`ÈëÏúĭçÐÂÎĂ
> >>>>:275F6E9B-FC45-4F3F-9BE5-745AC245C6DE@xxxxxxxxxxxxxxxxxxxx
> >>>>
> >>>>
> >>>>>"zengfeng" wrote:
> >>>>>
> >>>>>
> >>>>>>Does the privilege of system user can be modified?If can ,How to do
> >
> > it
> >
> >>?
> >>
> >>>>>What is "system user" – Local System?
> >>>>>
> >>>>>--
> >>>>>
> >>>>>
> >>>>>
> >>>>>
> >>>--
> >>>../ray\
> >>
> >
> >
>
> --
> ../ray\

.

- **References:**

- ◆ **system user**
 - ◇ From: zengfeng
- ◆ **RE: system user**
 - ◇ From: Pavel A.
- ◆ **Re: system user**
 - ◇ From: zengfeng
- ◆ **Re: system user**
 - ◇ From: Ray Trent
- ◆ **Re: system user**
 - ◇ From: Ray Trent
- ◆ **Re: system user**
 - ◇ From: zengfeng
- ◆ **Re: system user**
 - ◇ From: Ray Trent

- Prev by Date: **driver reload from kernel mode**
- Next by Date: **Driver Install using : DPIInst + amd64 + WIN XP 64**
- Previous by thread: **Re: system user**
- Next by thread: **Support for loading NIC firmware in NDIS**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**