

microsoft.public.inetserver.iis: Re: IIS 6.0 cgi process not running as same user as worker process?

## Re: IIS 6.0 cgi process not running as same user as worker process?

**Source:**

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-05/1301.html>

---

**From:** David Wang [Msft] (*someone\_at\_online.microsoft.com*)

**Date:** 05/12/04

Date: Wed, 12 May 2004 16:04:50 -0700

You definitely want to read documentation --- what you are doing is not "normal", so it requires you to understand some info which documentation provides.

IIS6 Resource Kit Tools --- Metabase Explorer:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLa>

IIS6 Commandline tools:

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/command\\_line\\_tools\\_included\\_in\\_iis.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/command_line_tools_included_in_iis.asp)

Documentation:

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref\\_mb\\_createprocessasuser.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref_mb_createprocessasuser.asp)

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref\\_mb\\_wamusername.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref_mb_wamusername.asp)

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref\\_mb\\_wamuserpass.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref_mb_wamuserpass.asp)

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref\\_mb\\_appoolidentitytype.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/iis/ref_mb_appoolidentitytype.asp)

--

//David

IIS

This posting is provided "AS IS" with no warranties, and confers no rights.

//

"Issac Goldstand" <isaac@cpan.org> wrote in message

news:u6DAJjGOEHA.640@TK2MSFTNGP12.phx.gbl...

How do I edit the metabase? I tried getting metaedit 2.2

It warns that it's intended for IIS 4 & 5... Is there an update or a better tool to use? Can I use it to connect to a remote metabase?

Also, I was thinking that the best place for me to edit the key is either in the AppPool (my 1st choice) or in the virtualdirectory (2nd choice). Must it be global?

Lastly, what are the Id and UserType fields - how should they be set?

Thanks for your help!

Issac

"David Wang [Msft]" <someone@online.microsoft.com> wrote in message

news:OWt4A8AOEHA.2876@TK2MSFTNGP09.phx.gbl...

> No... This is a frequently misunderstood feature.

>

> On Windows, executing code has both a thread token and a process token.

If

> the thread token is set (i.e. impersonated), then it is used to execute

> code; otherwise, the process token is used.

Re: IIS 6.0 cgi process not running as same user as worker process?

microsoft.public.inetserver.iis: Re: IIS 6.0 cgi process not running as same user as worker process?

>  
> The Application Pool Identity merely allows you to customize the process  
> token. It does not mean that IIS is going to execute all code on the  
server  
> using this identity.  
>  
> In fact, IIS executes code using impersonation by default, meaning the  
> identity that is executing the code comes from authentication (or IUSR in  
> the case of anonymous). This allows you to create users on NT and use IIS  
> to login as those users -- which allows IIS to leverage the rich  
> authentication/authorization infrastructure from NT. This is why CGIs are  
> launched using the impersonated identity.  
>  
> Prior IIS versions had a fixed "LocalSystem" as the process identity --  
not  
> exactly secure. Allowing the process token to be customizable is a form  
of  
> security lockdown since it represents a "sandbox" of maximum privilege  
that  
> code inside the AppPool can obtain. Users may authenticate and directly  
> elevate privileges (through impersonation), but any other code can only  
have  
> process identity... and IIS sets it to be a low-privileged Network Service  
> user by default, meaning that in the event of any exploitation, Network  
> Service is the identity... and not Local System.  
>  
> Now, script engines, CGI, and ISAPI may choose to use impersonation or  
> not -- for example, it is configurable to have IIS launch CGI as either  
the  
> impersonated user or process identity (it's controlled by a metabase  
> property, "CreateProcessAsUser", and it defaults to "1" [which means to  
> impersonate]), and ASP.Net also allows users to choose "impersonate" or  
not.  
>  
> In your case, I think you want to set "W3SVC/CreateProcessAsUser" property  
> to be 0. This will make your CGIs launch as app pool identity.  
>  
> --  
> //David  
> IIS  
> This posting is provided "AS IS" with no warranties, and confers no  
rights.  
> //  
> "Issac Goldstand" <isaac@cpan.org> wrote in message  
> news:OOESgZ5NEHA.3744@TK2MSFTNGP11.phx.gbl...  
> Hi list,  
> I've set up an application pool to run as a specific user which I set up  
> properly (member of IIS\_WPG, relevant security policy, relevant NTFS  
> permissions, etc). When I run a Perl CGI in this application pool, the  
w3wp  
> process runs as my user, but the Perl processes seems to be running as the  
> IUSR\_ user (which is the default anonymous access user for that app).  
Isn't  
> the whole idea of setting the application pool user to avoid this? I have  
> no problem with IUSR\_ user being used to serve static content, but why run  
> scripts?  
>  
> Very confused,  
> Issac  
>  
>  
>