

Re: xp_cmdshell default path (system32) problem

Source:

<http://www.tech-archive.net/Archive/SQL-Server/microsoft.public.sqlserver.programming/2009-06/msg00221.html>

- *From:* "Thomas Malia" <tommalia@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 2 Jun 2009 09:56:06 -0400
-

I sort of took this approach. Originally, some of my logic simply needed to purge all files from a given directory. So, the Logic was something like:

```
SET @CMD = 'del "' + @DIRNAME + '*.*'  
EXEC xp_cmdShell @CMD
```

This was the logic that was scaring the !@\$#%\$%#\$ out of me because if for any reason @DIRNAME ended up being an empty string, the command would have just deleted every file from C:\WINNT\SYSTEM32.... NOT a good thing!

So, I modified the logic so that it first does a DIR using a mask that would only select files ending in BAK and TRN (the files I want to purge and the only type of files that should ever be in the directory I'm trying to clean out). I put the result of that DIR into a temp table then use a cursor to cycle through that result set performing the deletes on the specific files. This way the deletes are never being done with a wild card so hopefully even if it does end up operating on SYSTEM32, it still wont delete any system files.

As I'm typing this though, I'm realizing I'm still leaving a hole. The Mask that should be used to identify the files that should be purged is maintained in a table and can be changed. I still have a potential problem if someone happens to change that mask to something like *.*. In that case the DIR simply generates the set of all records in the SYSTEM32 directory and I'm right back to the same problem I started with.

It still looks to me like, I can try like heck to put all kinds of safe guards in place and they will all help, but ultimately what I really need is a way to actually prevent xp_cmdshell from being allowed to do anything at all to certain directories. I keep coming back to needing a way to ensure that xp_cmdshell ALWAYS executes under the security context of defined windows user so that I can control access for that user. Is there any way to do this? I've used to PROXY account thing before, but my recollection was that, the Proxy account doesn't ALWAYS get used. It depends on what user context the SQL is script happens to be running under. Isn't there some way to just FORCE xp_cmdShell to ALWAYS use a particular windows account no matter what?

Re: xp_cmdshell default path (system32) problem

"Justin Rich" <jrich523@xxxxxxxxxxxxxxxx> wrote in message
news:e2Pwje34JHA.4272@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

simple :)

change your command from "dir path" to "if exist file del file"

this will check to see if its there, and if so, delete it

got to love good ol' dos :)

"Thomas Malia" <tommalia@xxxxxxxxxxxxxxxx> wrote in message
news:eh9NDlv4JHA.1716@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I'm trying to create some maintenance scripts that need to manage files in some directories. I want to purge files that are older than a given number of days. I'm use xp_cmdShell to execute "erase" command like commands to delete the files. The problem I'm concerned about is related to the fact that xp_cmdshell appears to use c:\WINNT\SYSTEM32 as it's default path.

I haven't executed the actual erase statements yet but rather have been running test where I just perform a DIR instead of a ERASE to confirm what WILL get deleted when I do it for real. The problem is, if the directory that I supply doesn't exist, then the command appears to operate on the "default path". So for example if I do:

```
EXEC xp_cmdshell 'DIR c:\MyDir'
```

and "myDir" doesn't actually exist, then the xp_cmdShell is return the same result set as if I executed:

```
EXEC xp_cmdshell 'DIR c:\WINNT\SYSTEM32'
```

This is more than a little scary since if I have had actually run this command with ERASE instead of DIR then presumably it would have deleted

all file from the C:\WINNT\SYSTEM32 directory.... BAD THING!

Now, I can be REALLY, REALLY careful when I write my scripts to make sure

I use an existing directory. However, this doesn't protect me later when my script is running as a scheduled job and some unsuspecting sole happens to delete, rename or change the security settings on my directory and now the next time the job runs I crush SYSTEM32!

There's got to be a better way to handle this... isn't there!?!

PLEASE HELP!

Re: xp_cmdshell default path (system32) problem