

# Re: Kerberos Problem with App Pool running as Domain Account

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2008-06/msg00067.html>

---

- *From:* "Consultant" <[consultant\\_mcngp@xxxxxxxxxx](mailto:consultant_mcngp@xxxxxxxxxx)>
  - *Date:* Mon, 23 Jun 2008 15:20:14 -0700
- 

is the domain account it is running under "trusted for delegation"?

"VC" <[VC@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:VC@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:3630E23B-1C39-48A9-BE3F-AB25507AE8A1@xxxxxxxxxxxxxxxxxxxx](mailto:news:3630E23B-1C39-48A9-BE3F-AB25507AE8A1@xxxxxxxxxxxxxxxxxxxx)

Thank you for the response.

There are some authentication types of "Negotiate" however, there are no duplicate SPNs, and as far as I can tell everything is setup as it should be.

My only thought might be that the application pool is running under a domain account, perhaps IIS itself has to as well (instead of the IUSR\_IISERVER account). But is this even supported, or likely to be the cause of the problem?

Here is an error from the security log:

Event Type: Failure Audit  
Event Source: Security  
Event Category: Logon/Logoff  
Event ID: 537  
Date: 6/23/2008  
Time: 10:36:56 AM  
User: NT AUTHORITY\SYSTEM  
Computer: IISSERVER  
Description:  
Logon Failure:  
Reason: An error occurred during logon  
User Name:  
Domain:  
Logon Type: 3  
Logon Process: Authz  
Authentication Package: Kerberos  
Workstation Name: IISSERVER  
Status code: 0xC000040A  
Substatus code: 0x0

Re: Kerberos Problem with App Pool running as Domain Account

Caller User Name: IISSERVER\$  
Caller Domain: TIB  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 1048  
Transited Services: –  
Source Network Address: –  
Source Port: –

And here's the negotiate authentication which occurs after:

Event Type: Success Audit  
Event Source: Security  
Event Category: Logon/Logoff  
Event ID: 528  
Date: 6/23/2008  
Time: 10:36:56 AM  
User: DOMAIN\USER  
Computer: IISSERVER  
Description:  
Successful Logon:  
User Name: user  
Domain: DOMAIN  
Logon ID: (0x0,0xA2489CC)  
Logon Type: 4  
Logon Process: Advapi  
Authentication Package: Negotiate  
Workstation Name: IISSERVER  
Logon GUID: {e241c991–82ad–2241–b533–510eff0f2c75}  
Caller User Name: IISSERVER\$  
Caller Domain: DOMAIN  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 840  
Transited Services: –  
Source Network Address: –  
Source Port: –

Any further help would be appreciated.

"Ken Schaefer" wrote:

a) you need to make sure that the browser is authenticating using Kerberos (and not NTLM). Check the Windows Event logs for this

b) you need to remove any duplicate SPNs you might have registered under the original computer account

<http://adopenstatic.com/faq> has a list of IIS and Kerberos articles that explain everything you need to do/check.

Re: Kerberos Problem with App Pool running as Domain Account

Cheers  
Ken

"VC" <VC@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:394285B1-438C-42D7-8EA8-D35CFAF63CD5@xxxxxxxxxxxxxxxxxxxx](mailto:news:394285B1-438C-42D7-8EA8-D35CFAF63CD5@xxxxxxxxxxxxxxxxxxxx)

Good Morning,

I have multiple applications running with integrated security to connect to a SQL back-end database. Everything works fine on our production servers which use the default system accounts for the Application Pool.

However, I had to change this to use a domain account because our DR server needed to work with the same DNS Alias which conflicted with the already registered SPNs.

As recommended, on our DR server, I began testing by changing the Application Pool to run under a domain account. I then registered the following SPNs:

```
setspn -A HTTP/iisserver domain\user  
setspn -A HTTP/iisserver.domain.com domain\user  
setspn -A MSSQLSvc/sqlserver:1433 domain\user
```

Additionally, I set the domain\user account to "Account is trusted for delegation" and the iisserver computer account to "Trust computer for delegation". Still, I receive the following error when connecting to the database:

Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'.

This works fine on the live server, so I'm assuming this is

Re: Kerberos Problem with App Pool running as Domain Account

related to  
changing the Application Pool to run under a domain  
account. Any  
suggestions  
would be greatly appreciated.

Thank you