

# Re: kerberos suddenly stop working on an IIS server

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-02/msg00505](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-02/msg00505)

---

- *From:* "Paul Williams [MVP]" <ptw2001@xxxxxxxxxxxx>
  - *Date:* Tue, 6 Feb 2007 21:15:54 -0000
- 

The following is cut and pasted from the MSFT Troubleshooting Kerberos whitepaper:

0xD – KDC\_ERR\_BADOPTION: KDC cannot accommodate requested option

Associated internal Windows error codes

.. STATUS\_NO\_MATCH

Corresponding debug output messages

.. DebugLog("Asked for forwarded but not allowed\n")

.. DebugLog("Asked for proxy but not allowed\n")

.. DebugLog("Asked for postdate but not allowed\n")

.. D\_DebugLog("s4u set, but no ticket\n")

.. D\_DebugLog("Couldn't decrypt evidence ticket %x\n")

.. D\_DebugLog("Trying to mix S4U proxy and self requests\n")

.. D\_DebugLog("KLIN(%x) Client %wZ sent AS request with no server name\n")

.. D\_DebugLog("KLIN(%x) Attempt made to renew non-renewable ticket\n")

.. DebugLog("Client tried to use pkinit w/o client cert\n")

.. DebugLog("User supplied bad cert type: %d\n")

Possible Causes and Resolutions:

.. Impending expiration of a TGT.

Resolution

Confirm the cause by verifying the expiration time on the TGT. To do this, use the Kerberos List parameter tgt. If you confirm that this is the cause, you need do nothing more, because the TGT will be automatically renewed or a new one will be requested if needed. For example, Windows XP and Windows Server 2003 will recover from this automatically.

.. The SPN to which the client is attempting to delegate credentials is not in its Allowed-to-delegate-to list.

Resolution

1. Use Network Monitor to determine the SPN to which the client is attempting to delegate credentials. You will need this information in a later step.
2. Click Start, click Run, and then open Active Directory Users and Computers by typing the following:  
dsa.msc
3. Right-click the user or service account that has problems authenticating, and then click Properties.
4. Click the Delegation tab.
5. The Allowed-to-delegate-to list is the list of servers shown under the heading, Services to which this account can present delegated credentials.
6. Add the SPN the client is attempting to delegate to (information from the captured data you obtained in Step 1) to the Allowed-to-delegate-to list for that client. This will tell the KDC that this client is indeed allowed to authenticate to this service. The KDC will then grant the client the appropriate ticket.

Re: kerberos sudenly stop working on an IIS server

For information about setting up service accounts for delegation, see "HOW TO: Configure Computer Accounts and User Accounts So That They Are Trusted for Delegation in Windows Server 2003 Enterprise Edition" in the Microsoft Knowledge Base at <http://go.microsoft.com/fwlink/?LinkId=23067>.

.. The server does not support constrained delegation or protocol transition. (Windows 2000 does not support constrained delegation or protocol transition.)

Out of curiosity, is this an x64 server?

--

Paul Williams

Microsoft MVP – Windows Server – Directory Services

<http://www.msresource.net> | <http://forums.msresource.net>

.