

Service Ticket Request Failure Audit

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-07/msg00830.html>

- *From:* "Ed" <JonesEJ@xxxxxxxx>
 - *Date:* 7 Jul 2006 08:58:21 -0700
-

I am receiving the following error every 15 minutes:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 673
Date: 7/7/2006
Time: 11:33:07 AM
User: NT AUTHORITY\SYSTEM
Computer: WINDJAMMER
Description:
Service Ticket Request:
User Name:
User Domain: << DOMAIN (i.e. thisdomain.local) >>>
Service Name: host/<< SBS ServerName >>.thisdomain.local
Service ID: -
Ticket Options: 0x40830000
Ticket Encryption Type: -
Client Address: 127.0.0.1
Failure Code: 0xD
Logon GUID: -
Transited Services: -

On eventid.net there was the following post:

Adrian Grigorof (Last update 5/7/2004):
The most common occurrence of this event has the following parameters:
- Ticket options: 0x40830000
- IP address: 127.0.0.1 (the localhost)
- Failure code: 0xD

The Kerberos ticket options refer to various flags that the requestor wants to set for the ticket. See the "Kerberos ticket options" article for the interpretation of various values that this field can take.

Failure code: 0xD (13 in decimal) = KDC cannot accommodate requested option (KDC_ERR_BADOPTION)

Service Ticket Request Failure Audit

Ticket option: 0x40830000, code: 0xD – From a newsgroup post: "This failure seems to indicate that an anonymous connection is being requested and denied. If you find this tightly coupled with a success then it may be that the client process simply first tries for a null session and then negotiates a secured one."

As per Microsoft, the "anonymous bit flag (bit 14) indicates that the principal is a generic domain account, such as anonymous, for the purpose of distributing a session key.

From a newsgroup post: "Technically speaking, the 673 Failure Audits

are due to users & computers with expired TGTs they are trying to renew. Please make sure that the time between the client and the server is synchronized. In addition, this issue may also occur if the client computer does not support S4U. Windows 2003 introduces support for constrained delegation which by leveraging the S4U2Proxy extension to Kerberos. The Kerberos client on a Windows 2003 server will regularly (every 15 minutes by default) check the KDC to see if it supports S4U. If the client doesn't support S4U, a failure security log will be recorded."

S4U = Service-for-User extensions

I have ensured that all clients and servers are synchronizing with the SBS server and the SBS server is configured to sync with time-a.nist.gov and all are within a negligible time difference no more than a second or 2. What i do not understand is the client ip of 127.0.0.1. All clients are running Win XP SP2 and the SBS server is 2003. There is a BDC that runs server 2003 std. Any help would be appreciated. Thank you.

.