

Re: Event ID 1030, 40961 and 673 on DC

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2006-05/msg00301.html>

- *From:* "Wills World" <wills@xxxxxxxxxxxxx>
 - *Date:* Sun, 7 May 2006 14:48:17 -0400
-

Although the KB article does not match exactly it is a close match to most of the symptoms.

MS Article ID : 885887
Last Review : April 27, 2006
Revision : 1.3

You cannot access network resources after you try to log on to a Windows XP Service Pack 2-based computer

Symptoms:

If you log on to a Microsoft Windows XP Service Pack 2 (SP2)-based computer before a domain controller on your network is available, you may experience one or more of the following symptoms:

- .. User-specific Kerberos Ticket-Granting Tickets (TGT) are not renewed.
- .. Requests for new TGTs are not accepted if the TGT has reached its last permissible renew date after you install Windows XP SP2.
- .. Authentication to network resources may unexpectedly quit after the computer has been locked.
- .. Programs that use Delegation may unexpectedly quit.
- .. You cannot resolve the problem by purging the TGT and requesting a new TGT.
- .. You find an event similar to the following event in the system event log:

Event Type: Warning
Event Source: LSASRV
Event Category: SPNEGO (Negotiator)
Event ID: 40961
Date: 10/27/2004
Time: 1:00:50 PM
User: N/A
Computer: COMPUTER
Description: The Security System could not establish a secured connection with the server ldap/DC01.corp.com/corp.com@xxxxxxxx No authentication protocol was available.

To Get the Hot Fix Mentioned in the KB Article:

I called 1-800-MICROSOFT (1-800-642-7676) and followed the telephone prompts to get a HotFix. I got transferred to a real person who simply asked what Hot Fix I needed and then they emailed it to me with a password.

I have installed the Hot Fix on one machine and will post back the results.

"Wills World" <wills@xxxxxxxxxxxx> wrote in message
news:%23Xi952WbGHA.3364@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Windows 2003 SP1 Domain 3 DC's
Windows XP SP2

Details of Problem:

Event logs of XP Clients are reporting the events 1030 (USERENV) and 40961 (LSASRV/SPNEGO) only when the users machine is logged in but locked. (After they go home) The events seem to happen about every two hours until they unlock and then the problem stops again.

Domain Controller Log reports event 673 Failure With no Username/Domain/Service Name/Service ID

Ticket Options: 0x2
Client Address: (matches the clients ip address)
Failure Code 0X20 (Ticket Expired?)

Can you explain what might be happening here and possible solutions?