

FIXED!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-06/0776.html>

From: Donald P. Crawford (*crawford_at_ksu.edu*)

Date: 06/11/03

Date: Wed, 11 Jun 2003 08:02:57 -0700

Thanks, Steven!

Running netdiag on the client gave me a few more clues.
This is what I found and after applying the reg
modification, the problem appears to be resolved.

Thanks again!

Microsoft Knowledge Base Article – 244474
How to Force Kerberos to Use TCP Instead of UDP
The information in this article applies to:
Microsoft Windows 2000 Server
Microsoft Windows 2000 Advanced Server
Microsoft Windows 2000 Professional
Microsoft Windows 2000 Datacenter Server
Microsoft Windows XP Professional

This article was previously published under Q244474
IMPORTANT: This article contains information about
modifying the registry. Before you modify the registry,
make sure to back it up and make sure that you understand
how to restore the registry if a problem occurs. For
information about how to back up, restore, and edit the
registry, click the following article number to view the
article in the Microsoft Knowledge Base:
256986 Description of the Microsoft Windows Registry

SUMMARY

The Windows Kerberos Authentication package is the
default in Windows 2000 and Windows XP. It coexists with
challenge/response (NTLM) and is used in instances in
which both a client and server can negotiate Kerberos.
Request for Comments (RFC) 1510 states that when a client
contacts the Key Distribution Center (KDC), it should
send a User Datagram Protocol (UDP) datagram to port 88
at the KDC's IP address. The KDC should respond with a
reply datagram to the sending port at the sender's IP

FIXED!

address. The RFC also states that UDP must be the first protocol tried.

The limitation on the UDP packet size may result in the following error message at domain logon:

Event Log Error 5719
Source NETLOGON

No Windows NT or Windows 2000 Domain Controller is available for domain Domain. The following error occurred:

There are currently no logon servers available to service the logon request.
You may also get the following errors from Netdiag.

DC list test : Failed [WARNING]
Cannot call DsBind to COMPUTERNAMEDC.domain.com
(159.140.176.32). [ERROR_DOMAIN_CONTROLLER_NOT_FOUND]

Kerberos test. : Failed [FATAL]
Kerberos does not have a ticket for MEMBERSERVER\$.]
MORE INFORMATION

WARNING: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

By default, Windows 2000 and Windows XP use UDP when the data can be fit in packets under 2,000 bytes. Any data above this value uses TCP to carry the packets. The value of 2,000 bytes is configurable by modifying a registry key and value.

Start Registry Editor.

Locate and then click the following key in the registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

If the Parameters key does not exist, you can create it now.

On the Edit menu, click Add Value, and then add the following registry value:

Value Name: MaxPacketSize

Data Type: REG_DWORD

Value: any integer value in the range 1 to 2000 (in bytes)

Quit Registry Editor.

Restart your computer.

The data value to which you set this value is the maximum

size to be used with UDP. If the packet size exceeds this value, TCP is used. Again, 2,000 bytes is the default if the value is not present.

To prevent UDP from ever being used, set the value to 1; TCP will be used for all packets. Forcing TCP packets only is an effective workaround to this problem.

The following is an Administrative Template that can be imported into Group Policy to allow this value to be set for all the Windows 2000-based or Windows XP-based computers in the enterprise. CLASS MACHINE

CATEGORY !!KRB_PARAMS

KEYNAME "SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters"

POLICY !!SET_MAXPACKETSIZE
EXPLAIN !!MAXPACKETSIZE_HELP
PART !!MAXPACKETSIZE_NUMERIC_REQUIRED
VALUENAME "MaxPacketSize"
MIN 1 MAX 2000 DEFAULT 2000
END PART

PART !!MAXPACKETSIZE_TIP_TEXT
END PART
END POLICY

POLICY !!LOGLEVEL
EXPLAIN !!LOGLEVEL_HELP
VALUENAME "LogLevel"
END POLICY
END CATEGORY

[strings]
KRB_PARAMS="Kerberos Parameters"
SET_MAXPACKETSIZE="Set MaxPacketSize"
MAXPACKETSIZE_HELP="The Windows 2000 Kerberos Authentication package is the default in Windows 2000. It coexists with challenge/response (NTLM) and is used in instances in which both a client and server can negotiate Kerberos. Request for Comments (RFC) 1510 states that when a client contacts the Key Distribution Center (KDC), it should send a User Datagram Protocol (UDP) datagram to port 88 at the KDC's IP address. The KDC should respond with a reply datagram to the

FIXED!

sending port at the sender's IP address.\n\nWindows 2000, by default, uses UDP when the data can be fit in packets under 2,000 bytes. Any data above this value uses TCP to carry the packets. The value of 2,000 bytes is configurable via this policy."
MAXPACKETSIZE="Bytes: "
MAXPACKETSIZE_TIP="Range is from 1 to 2000. Use 1 to force Kerberos to use TCP."
LOGLEVEL="Kerberos Event Logging"
LOGLEVEL_HELP="Windows 2000 offers the capability of tracing detailed Kerberos events through the event log mechanism. You can use this information when you troubleshoot Kerberos. All Kerberos errors are logged to the System log."

For additional information, click the article number below to view the article in the Microsoft Knowledge Base:
320903 Clients Cannot Log On by Using Kerberos over TCP

Last Reviewed: 6/11/2003
Keywords: kbenv kbinfo KB244474