

Re: JCIFS18_15_5D

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2008-05/msg00413.html>

- *From:* Meinolf Weber <meiweb(nospam)@gmx.de>
 - *Date:* Thu, 8 May 2008 12:48:28 +0000 (UTC)
-

Hello Charles,

Please post the complete event log, just press the 2 paper button in the right corner and paste it to the posting, so the complete error is here. This names will be no service from authentication or something else, this specifies machine names.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! http://www.blakjak.demon.co.uk/mul_crss.htm

Below is the text from the event log:

The domain controller attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Logon Account: MAGREL

Source Workstation: \\JCIFS18_143_B5

Error Code: 0xc000006a

Yes, we checked the DNS and the names were not in there. We also have a Cisco wireless network where we searched for the PC names but did not find them. No...this is not a naming convention for our network.

This is the first time we were unable to locate a host on our network which is why we thought that these names may be legitimate services attempting to authenticate since the user name "MAGREL" is a legitimate user name used by services on some of our servers (the ones that required a reboot from the Windows updates). Also, remember that the issued went away after we rebooted the servers.

Here are a few of the source names we found:

JCIFS18_143_B5

JCIFS18_15_5d

Re: JCIFS18_15_5D

JCIFS18_145_ed

As you can see, all of the mystery names begin with JCIFS18. Is this the format used by Windows for services attempting to authenticat to domain controllers? Please verify. From the above names, it appears that this is a naming convention used by some OS or service. Does anyone recognise this naming convention?

Thanks.

"Meinolf Weber" wrote:

Hello Charles,

Please post the complete event viewer entry where these names are stated.

Also did you check DNS for them? Is the naming according to your internal naming convention?

And ofcourse you should reboot the servers after installing patches, so that

also registry keys could update for example, otherwise some patches have

no effect.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers

no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! http://www.blakjak.demon.co.uk/mul_crss.htm

We had a few Windows servers that had the last batch of Windows Updates installed and were not rebooted (there was a box indicating that a reboot was required on the desktop). We noticed that a user account that is used on many services on these servers was getting locked out on the domain controllers every couple of minutes. We finally resolved the issue by rebooting the servers.

What makes this odd is that the source of the authentication request awas from JCIFS18_15_5D and JCIFS18_145_ED. These machines do not exist on our network. We scanned our network and did not find them.

Re: JCIFS18_15_5D

Re: JCIFS18_15_5D

We did a NETSTAT -a and no host was found.

My question is this:

Does anyone know what JCIFS18_15_5D is? We're thinking that maybe these are IDs for services that were attempting to authenticate to the DCs. Could someone verify this?

Thanks.