

Re: Cannot request computer certificate.

> node first while ADS&S is highlighted. In security for the CA everyone
> should have read and special permissions. I am running out of ideas also :
> (--- Steve
>
>
> tp://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx ---
> Windows 2003 PKI resources.
>
> "Jarryd" <j@xxx> wrote in message
> news:O3rNGwvEGHA.2300@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> Hi Steve,
>>
>> I was so hoping you were going to reply. Right to answer your questions:
>>
>> Q.) What operating system and what type of CA are you using?
>> A.) Windows Server 2003 SP1
>> Q.) Is this a new or ongoing problem?
>> A.) First time I have encountered it. Then again I haven't needed to
>> request a computer certificate for about 9 months.
>> Q.) More than one domain in the forest?
>> A.) Just the one. Very simple setup.
>> Q.) I would first verify that the CA is running, logon to it as an admin
>> and verify that you can get a computer/server certificate from it.
>> A.) The CA is running. I can log on to it. I cannot get a
>> computer/server certificate from it – that is my problem. But the server
>> can successfully request a certificate for itself.
>> Q.) You can also use certutil to check on the CA such as certutil –ping
>> at least for Windows 2003.
>> A.) Result:
>> -----
>> H:\>certutil –ping
>> 402.203.0: 0x80070057 (WIN32: 87): ..CertCli Version
>> 417.329.0: 0x80070103 (WIN32: 259)
>> 417.596.0: 0x80070103 (WIN32: 259)
>> 410.2618.0: 0x80070002 (WIN32: 2)
>> 410.2633.0: 0x80070103 (WIN32: 259)
>> CertUtil: No local Certification Authority; use –config option
>> 301.2585.0: 0x80070103 (WIN32: 259)
>> 301.2824.0: 0x80070103 (WIN32: 259)
>> CertUtil: No more data is available.
>> 301.3128.0: 0x80070103 (WIN32: 259)
>> -----
>> Q.) Verify that you can ping it by name and IP address from the client
>> computers.
>> A.) Ping OK.
>> Q.) In the CA Management Console look in properties for your CA and go to
>> security and verify that authenticated users have request certificates
>> permission.
>> A.) They do, along with read permission. I have also explicitly given
>> myself, my PC, and the server having the problem all four permissions.
>> Still no luck.

Re: Cannot request computer certificate.

Re: Cannot request computer certificate.

>> Q.) If you are using Windows 2003 see if there is any info in failed
>> requests.
>> A.) Nothing failed.
>> Q.) Look in the logs of the CA via Event Viewer,etc. to see if there any
>> pertinent messages there including any that may show errors for Group
>> Policy.
>> A.) Nothing in event viewer.
>> Q.) Possibly there is a problem with the CA or domain computers
>> contacting domain controllers.
>> A.) The CA is a domain controller. I have no error messages when logging
>> on, and nothing in event viewer to that effect either.
>> Q.) An Enterprise CA needs to be trusted for delegation I believe so
>> check it's computer account in Active Directory Users and Computer for
>> that and to make sure that computer is in the
>> A.) The Enterprise CA is trusted for delegation and it is a member of
>> CERTSVC_DCOM_ACCESS and Cert Publishers groups.
>> Q.) I would run the support tool netdiag on your domain controller [at
>> least pdc fsmo], your CA, and a client domain computer having a problem
>> looking for any errors/warnings relating to dc discovery, secure channel,
>> Kerberos, or dns.
>> A.) Results:
>> 1.) Client:
>> -----
>> Netcard queries test : Passed
>>
>> Per interface results:
>>
>> Adapter : Local Area Connection
>>
>> Netcard queries test . . . : Passed
>>
>> Host Name. : IT1.domain.com
>> IP Address : 200.200.10.18
>> Subnet Mask. : 255.255.255.0
>> Default Gateway. : 200.200.10.254
>> Primary WINS Server. . . . : 200.200.10.1
>> Dns Servers. : 200.200.10.2
>> 200.200.10.3
>>
>> AutoConfiguration results. : Passed
>>
>> Default gateway test . . . : Passed
>>
>> NetBT name test. : Passed
>> [WARNING] At least one of the <00> 'WorkStation Service', <03>
>> 'Messenger Service', <20> 'WINS' names is missing.
>>
>> WINS service test. : Passed
>>
>>
>> Global results:

Re: Cannot request computer certificate.

Re: Cannot request computer certificate.

```
>>
>> Domain membership test . . . . . : Passed
>>
>> NetBT transports test. . . . . : Passed
>> List of NetBt transports currently configured:
>> NetBT_Tcpip_{F3401C24-6574-42C3-AC4E-D74FAC611C8D}
>> 1 NetBt transport currently configured.
>>
>> Autonet address test . . . . . : Passed
>>
>> IP loopback ping test. . . . . : Passed
>>
>> Default gateway test . . . . . : Passed
>>
>> NetBT name test. . . . . : Passed
>> [WARNING] You don't have a single interface with the <00> 'WorkStation
>> Servi
>> ce', <03> 'Messenger Service', <20> 'WINS' names defined.
>>
>> Winsock test . . . . . : Passed
>>
>> DNS test . . . . . : Passed
>>
>> Redir and Browser test . . . . . : Passed
>> List of NetBt transports currently bound to the Redir
>> NetBT_Tcpip_{F3401C24-6574-42C3-AC4E-D74FAC611C8D}
>> The redir is bound to 1 NetBt transport.
>>
>> List of NetBt transports currently bound to the browser
>> NetBT_Tcpip_{F3401C24-6574-42C3-AC4E-D74FAC611C8D}
>> The browser is bound to 1 NetBt transport.
>>
>> DC discovery test. . . . . : Passed
>>
>> DC list test . . . . . : Passed
>>
>> Trust relationship test. . . . . : Passed
>> Secure channel for domain 'Domain' is to '\\srvr3.domain.com'.
>>
>> Kerberos test. . . . . : Passed
>>
>> LDAP test. . . . . : Passed
>> [WARNING] Failed to query SPN registration on DC 'srvr3.domain.com'.
>> [WARNING] Failed to query SPN registration on DC 'srvr2.domain.com'.
>>
>> Bindings test. . . . . : Passed
>>
>> WAN configuration test . . . . . : Skipped
>> No active remote access connections.
>>
>> Modem diagnostics test . . . . . : Passed
```

Re: Cannot request computer certificate.

Re: Cannot request computer certificate.

```
>>
>> IP Security test . . . . . : Passed
>> Service status is: Started
>> Service startup is: Automatic
>> IPSec service is available, but no policy is assigned or active
>> Note: run "ipseccmd /?" for more detailed information
>>
>> The command completed successfully
>> -----
>> 2.) CA (which is also the also the PDC FSMO)
>> .....
>>
>> Computer Name: SRVR3
>> DNS Host Name: srvr3.domain.com
>> System info : Windows 2000 Server (Build 3790)
>> Processor : x86 Family 15 Model 2 Stepping 9, GenuineIntel
>>
>> Netcard queries test . . . . . : Passed
>>
>> Per interface results:
>>
>> Adapter : Local Area Connection
>>
>> Netcard queries test . . . : Passed
>>
>> Host Name. . . . . : srvr3
>> IP Address . . . . . : 200.200.10.3
>> Subnet Mask. . . . . : 255.255.255.0
>> Default Gateway. . . . . : 200.200.10.254
>> Dns Servers. . . . . : 200.200.10.2
>> 200.200.10.3
>>
>> AutoConfiguration results. . . . . : Passed
>> Default gateway test . . . : Passed
>> NetBT name test. . . . . : Passed
>> WINS service test. . . . . : Skipped
>> There are no WINS servers configured for this interface.
>>
>> Global results:
>>
>> Domain membership test . . . . . : Passed
>>
>> NetBT transports test. . . . . : Passed
>> List of NetBt transports currently configured:
>> NetBT_Tcpip_{FF77261C-B517-468C-9244-E3EABC4C12FD}
>> 1 NetBt transport currently configured.
>>
>> Autonet address test . . . . . : Passed
>>
>> IP loopback ping test. . . . . : Passed
>>
```

Re: Cannot request computer certificate.

Re: Cannot request computer certificate.

```
>> Default gateway test . . . . . : Passed
>>
>> NetBT name test. . . . . : Passed
>>
>> Winsock test . . . . . : Passed
>>
>> DNS test . . . . . : Passed
>> PASS – All the DNS entries for DC are registered on DNS server
>> '200.200.10.2
>> ' and other DCs also have some of the names registered.
>> PASS – All the DNS entries for DC are registered on DNS server
>> '200.200.10.3
>> ' and other DCs also have some of the names registered.
>>
>> Redir and Browser test . . . . . : Passed
>> List of NetBt transports currently bound to the Redir
>> NetBT_Tcpip_{FF77261C-B517-468C-9244-E3EABC4C12FD}
>> The redir is bound to 1 NetBt transport.
>>
>> List of NetBt transports currently bound to the browser
>> NetBT_Tcpip_{FF77261C-B517-468C-9244-E3EABC4C12FD}
>> The browser is bound to 1 NetBt transport.
>>
>> DC discovery test. . . . . : Passed
>>
>> DC list test . . . . . : Passed
>>
>> Trust relationship test. . . . . : Skipped
>>
>> Kerberos test. . . . . : Passed
>>
>> LDAP test. . . . . : Passed
>>
>> Bindings test. . . . . : Passed
>>
>> WAN configuration test . . . . . : Skipped
>> No active remote access connections.
>>
>> Modem diagnostics test . . . . . : Passed
>> IP Security test . . . . . : Skipped
>> Note: run "netsh ipsec dynamic show /?" for more detailed information
>>
>> The command completed successfully
>>
```

```
>> Q.) If the CA is Windows 2003 and you have the Windows Firewall enabled
>> then disable it at least temporarily until the problem is resolved
>> assuming this will not expose it to untrusted networks such as the
>> internet.
>> A.) Already disabled.
>> Q.) Review the link below on Active Directory dns to make sure that your
```

Re: Cannot request computer certificate.

Re: Cannot request computer certificate.

>> dns is correctly configured for the domain.
>> A.) As far as I can tell DNS is tip top.
>> Q.) You could also try Web Enrollment to see if that works or not for
>> now.
>> A.) Web enrollment does work, but I can't get a computer (Client
>> Authentication) certificate using the web enrollment.
>>
>> So I really am stumped. Is there not a common reason why this doesn't
>> work. I have installed a new server in a test network (1 x server = DC +
>> CA), and connected one client to it. I have the same problem in the test
>> network. What have I not done. The strange thing is that this was
>> working. I really feel like I am going to have a break down. I might
>> even just run away and never come back.
>>
>> Please help!!
>>
>> TIA,
>>
>> Jarryd
>>
>> "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:%23YdiHlvEGHA.3984@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>> What operating system and what type of CA are you using? More than one
>>> domain in the forest? Is this a new or ongoing problem? I would first
>>> verify that the CA is running, logon to it as an admin and verify that
>>> you can get a computer/server certificate from it. You can also use
>>> certutil to check on the CA such as certutil -ping at least for Windows
>>> 2003. Verify that you can ping it by name and IP address from the client
>>> computers. In the CA Management Console look in properties for your CA
>>> and go to security and verify that authenticated users have request
>>> certificates permission. If you are using Windows 2003 see if there is
>>> any info in failed requests. Look in the logs of the CA via Event
>>> Viewer,etc. to see if there any pertinent messages there including any
>>> that may show errors for Group Policy. Possibly there is a problem with
>>> the CA or domain computers contacting domain controllers. An Enterprise
>>> CA needs to be trusted for delegation I believe so check it's computer
>>> account in Active Directory Users and Computer for that and to make sure
>>> that computer is in the
>>>
>>> I would run the support tool netdiag on your domain controller [at least
>>> pdc fsmo], your CA, and a client domain computer having a problem
>>> looking for any errors/warnings relating to dc discovery, secure
>>> channel, Kerberos, or dns. If you have multiple domain controllers run
>>> dcdiag and gpoutil on at least the pdc fsmo. If the CA is Windows 2003
>>> and you have the Windows Firewall enabled then disable it at least
>>> temporarily until the problem is resolved assuming this will not expose
>>> it to untrusted networks such as the internet. Review the link below on
>>> Active Directory dns to make sure that your dns is correctly configured
>>> for the domain. You could also try Web Enrollment to see if that works
>>> or not for now. --- Steve
>>>

Re: Cannot request computer certificate.

Re: Cannot request computer certificate.

◇ *From:* Jarryd

• **References:**

◆ **Cannot request computer certificate.**

◇ *From:* Jarryd

◆ **Re: Cannot request computer certificate.**

◇ *From:* Steven L Umbach

◆ **Re: Cannot request computer certificate.**

◇ *From:* Jarryd

◆ **Re: Cannot request computer certificate.**

◇ *From:* Steven L Umbach

• Prev by Date: **Re: Cannot request computer certificate.**

• Next by Date: **Re: User can't connect to particular webserver from his PC.**

• Previous by thread: **Re: Cannot request computer certificate.**

• Next by thread: **Re: Cannot request computer certificate.**

• Index(es):

◆ **Date**

◆ **Thread**