Windows Server Troubleshooting: RPC serv unavailable

Table of Contents

Introduction

Remote Procedure Call (RPC) is an inter-process communication technique to allow client and server software to communi based on a client/server model. The client makes a procedure call that appears to be local but is actually run on a remote c call arguments are bundled and passed through the network to the server. The arguments are then unpacked and run on t passed back to the client, where it is converted to a return value for the client's procedure call.

RPC is used by several components in Windows Server, such as the File Replication Service (FRS), Active Directory Replicati DCPromo and RDP, NLB and Cluster, Microsoft Operations Master, Exchange and SQL.

The RPC Server

An RPC server is a communications interface provided by an application or service that allows remote clients to connect, p RPC protocol. A typical example of an RPC server is Microsoft Exchange Server. Microsoft Exchange Server is an applicatior RPC communications interface for an RPC client.

An application will register its RPC server with the operating system's End Point Mapper (EPM) service so that the remote c application registers with the EPM it will indicate the IP address and TCP port that it is listening on.

The RPC Client

An RPC client is an application running on any given computer that uses the RPC protocol to communicate with an RPC se the Microsoft Outlook application.

NOTE: In this document the terms **RPC server** and **RPC client** refer to the **application** running at both ends of an RPC co

↑ Back to top

RPC Quick Fixes

Common causes of RPC errors include:

- Errors resolving a DNS or NetBIOS name.
- The RPC service or related services may not be running.
- number of connectivity Problems with network connectivity.
- File and printer sharing is not enabled.

Use the following procedures to diagnose and repair common causes of RPC errors.

Unable to resolve DNS or NetBIOS names in an Active Directory environm

1. Use the following commands to verify DNS is working for all DC's or specific DC's:
    - To get a DNS status for all DCs in forest, run the following command:
        - DCDIAG /TEST:DNS /V /E /F:<filename.log>
        - The "/e" switch runs the DNS test against all DCs in an Active Directory Forest
    - To get DNS health on a single DC, run the command below.
        - DCDIAG /TEST:DNS /V /S:<DCNAME> /F:<filename.log>
        - The "/s:" switch runs the DNS test against a specified domain controller.
    - To verify that a domain controller can be located for a specific domain, run the command below.
        - NLTEST /DSGETDC:<NetBIOS or DNS domain name>

1. Servers and clients that are receiving the error should be checked to verify that they are configured with the approp pointing to their ISP's DNS servers in the preferred or alternate DNS server portion of the TCP/IP settings. The ISP's forwarders in DNS.

1. Ensure that at least one correct DNS record is registered on each domain controller.
    - To ensure that a correct DNS record is registered on each domain controller, find this server's Active Director
    - Open DNSManager and connect in turn to each of these replication partners.
    - Find the host (A) resource record registration for this server on each of the other replication partner domain
    - Delete those host (A) records that do not have IP addresses corresponding to any of this server's IP addresse
    - If a domain controller has no host (A) records for this server, add at least one that corresponds to an IP addre addresses for this server, add at least one that is on the same network as the domain controller you are upda

1. Name resolution may also fail with the RPC Server is unavailable error if NetBIOS over TCP/IP is disabled on the WIN properties. The NetBIOS over TCP/IP setting should be either enabled or default (use DHCP).

1. Verify that a single label domain name is not being configured. DNS names that do not contain a suffix such as .con be single-label DNS names. Microsoft doesn't recommend using single label domain names because they cannot b domain members do not perform dynamic updates to single-label DNS zones. Knowledge base article 826743 - " records in a single-label domain" provides instructions on how to configure your domain to allow dynamic registrat

The RPC service or related services may not be started

Verify the status and startup type for the RPC and RPC locator services on the server that gets the error:

1. By default, Windows server 2003 domain controllers and member servers all should have the RPC service started an Locator service stopped and set to Manual Startup.
2. Windows 2000 domain controllers should have the RPC and RPC Locator services both set to started and automatic servers should have the RPC service started and set to automatic startup while the RPC locator service should be sta
3. If you make any changes to the RPC service or to the RPC Locator service settings, restart the computer, and then te
4. Additional Services that may result in "The RPC Server is Unavailable" errors are the TCP/IP NetBIOS helper service, I Registry service. These services should both be set to automatic and started. The Kerberos Key Distribution Center (I Windows 2000 and Windows 2003 DCs. It should not be started and set to Disabled in all other cases.

↑ Back to top

Network Connectivity

Verify ports needed by RPC are open

Verify that ports greater than 1024 are not blocked. Clients connect to RPC Endpoint Mapper on port 135. RPC Endpoint M assigned port between 1024-65535 a requested service is listening on.

Ports may be blocked by a hardware firewall or a software firewall. Software firewalls include Internet Connection Firewall c or Windows XP, and Windows Firewall on computers running Windows Vista, Windows 7, Windows Server 2008 and Windo

have third-party firewall software installed, or antivirus software with built-in firewall functionality. By default, port 135 TCP open for RPC to work. You can restrict the ports greater than 1024 that RPC uses. However, RPC Endpoint Mapper is alway

File and Printer Sharing is not enabled

File and Printer sharing for Microsoft Networks will produce the error RPC Server is unavailable" when you try to view or m the Services snap-in. See the following example:

Unable to open service control manager database on \\<computer>.

Error 1722: The RPC server is unavailable.

This error message may occur if the File and Printer Sharing for Microsoft Networks component is not enabled on the rem

Troubleshooting RPC

The process of an RPC client connecting to an RPC server can be broken down into four phases. This troubleshooting guid phase, how to test these events, and how to identify if the phase completed successfully.

Phase 1: Name Resolution: Name resolution is the act of resolving a name to an IP address. This normally takes two form common DNS Name Resolution.

Phase 2: TCP session establishment: TCP session establishment is the act of establishing a TCP connection between the F will be initiated by the RPC client via a TCP 3-way handshake with the RPC server.

Phase 3: RPC Discovery: When a client wants to connect to the RPC server supplied by the application it will contact the c discover how to connect to the RPC Server.

Phase 4: RPC Communication: RPC Communication is the act of making RPC requests to the application endpoint and re

<u>Data needed to troubleshoot the issue:</u>

- Identify the client and server computers reporting the RPC error. Identify the DNS and WINS servers used by these c
  - On each machine, open a command prompt and run **ipconfig /all**.
  - Determine the IP address of both machines. If the server is part of a cluster get the cluster resource IP addre WINS servers that the RPC client is configured to use.

Note: You can also obtain this information by opening **Control Panel\Network and Sharing Center,** clicking Local Area C

- Identify the application(s) reporting RPC Server Unavailable
- Simultaneous network traces (using Wireshark, Netmon, or a comparable network sniffer) from the machines hostin reproducing the task that results in a "RPC Server Unavailable" error.
  - The network captures on both hosts should be started first.
  - From a command prompt on the client run ipconfig /flushdns and nbtstat –R to clear the name resolution ca
  - Reproduce the error.
  - Stop the traces and save them.

↑ Back to top

Name Resolution

Name Resolution consists of one or possibly more NetBIOS or DNS queries to locate the IP address for the RPC Server. Tro that a response is received to the name resolution request and that the response contains the correct IP address for the RF by DNS or NetBIOS in the network trace for the server with the IP addresses you noted earlier. If it does not match then ch difference.

DNS Name Resolution

To identify DNS Name Resolution in a network trace use the following filter in Network Monitor or Wireshark: dns. DNS res open the network trace taken from the RPC client machine. You will be looking for one packet that is the query from the cl response packet from the DNS server. It will look similar to this:

If the trace shows the correct IP address for the RPC server was returned by the DNS server proceed to TCP Session Establi

If the trace does not show a correct IP address returned or you do not see any answer from the DNS server then reference name resolution troubleshooting.

For details on troubleshooting Active Directory related DNS issues go here.

For general DNS troubleshooting: http://support.microsoft.com/default.aspx?scid=kb;EN-US;330511

NetBIOS Name Resolution

NetBIOS queries come in two forms, WINS or NetBIOS Broadcasts. WINS will consist of a unicast query to a WINS server ar

NetBIOS broadcasts are queries broadcast to all hosts on the local subnet so name resolution is limited to only hosts on th the NetBIOS Broadcast will respond with its IP address.

To identify NetBIOS Name Resolution in a network trace, use the following filter in Network Monitor - "nbtns". For Wiresh trace shows a successful resolution using WINS or NetBIOS queries proceed to TCP Session Establishment.

For details on troubleshooting this NetBIOS Name Resolution further:

http://technet.microsoft.com/en-us/library/cc940110.aspx

TCP Session Establishment

TCP Sessions always begin with a TCP 3-way handshake. The handshake should look similar to what is shown below. The R the SYN packet. The computer hosting the RPC Server will send a SYN/ACK response, and then the RPC Client will send ar

Scenarios that may cause the TCP session to fail

Firewall/Network

If a firewall or network problem is the culprit, it is likely a failure will occur during this phase. To diagnose this you will want the RPC Client and RPC Server. If a firewall or other network device is causing a problem it will usually manifest as a retrans about 3 seconds after the first TCP SYN is sent. This can be seen in a Netmon network trace using the display filter specific cases, firewalls will allow the 3-way handshake to succeed but may block the RPC packets due to the contents of the packe possible to see the retransmit of the RPC packet within half a second of the original packet being sent. To identify this con display filter specification of "tcpretransmit==1". To see either of these retransmit conditions in a trace taken using Wiresh "tcp.analysis.retransmission".

The RPC Server is not actively listening.

It was noted earlier that an RPC Server will register itself and listen on a particular port and IP address of the host compute will answer the SYN packet from the client with a Reset packet.

A device in the middle between the RPC Client and RPC Server will be resetting the connection attempt.

In the client side trace it will appear as if the server sent the TCP Reset while the trace from the server indicates the client is

For both these scenarios, check for the presence of a Reset packet in the TCP three way handshake by using the display filt

For troubleshooting this step see the following sections in this document:

- How to identify RPC traffic in a trace

- Connectivity
- RPC Services
- RPC Client Registry

If the 3-way handshake is successful, continue to the **RPC Discovery** phase.

↑ Back to top

RPC Discovery

The RPC Discovery phase will occur one of two ways. In both methods the client will know the identifier for the RPC Server the computer hosting the RPC Server and ask for information on how to contact the RPC Server. The identifier is different RPC client will know ahead of time which method it wishes to use.

Discovery - RPC Over TCPIP

This method is a two-step process. First the RPC client will contact the End Point Mapper (EPM) on the machine hosting th address that Server is listening on. Upon successful completion of this the RPC client will contact the RPC Server directly o a sample of what this would look like and a step by step explanation below it. This step depends on the successful TCP ses and then to the RPC Server.

1. The RPC Client will open a TCP session with TCP port 135 on the computer hosting RPC Server of interest. This can b syntax in Netmon or Wireshark: "tcp.port==135"
2. The RPC Client will send an RPC Bind request using the UUID of the End Point Mapper and the RPC EPM should res
3. The RPC Client will make a MAP request to the EPM to locate the IP address and port of the RPC Server of interest, UUID.
4. The EPM will send back a MAP Response that indicates the IP and port the RPC Server is listening on.
5. The RPC Client will then open a TCP session with the IP and port it received in the EPM MAP response.
6. The client will send an RPC Bind Request to the RPC Server specifying the UUID of the RPC Server application and sl Server.
7. There will be an RPC Alter Context Request/Response in which authentication will take place. If an error is noted he determining why the error is occurring - Authentication
8. Perform some RPC operations...(Go to RPC Communication phase)

Discovery - RPC Over SMB

The second method an RPC Client may use to contact an RPC Server is RPC over SMB. This method depends upon first est hosting the RPC Server and then using the Named Pipes protocol to communicate using RPC. So in effect there are severa Pipes over SMB over TCP. We will not address the SMB session setup in this document and the TCP session establishment

With a successfully opened TCP and SMB session, next:

1. The RPC Client will issue a SMB TreeConnectAndX for the tree name "IPC$". This is a special hidden share for inter-p positive response from the computer hosting the RPC Server.
2. The RPC Client will then issue an SMB NTCreateAndX for the name of the PIPE of the RPC Server Application and sh examples are:

EVENTLOG = The Event log service

winreg = Remote Registry

svcctl = Service Control Manager

srvsvc = Server Service

1. Next there is a Bind handshake. This is to "bind" the RPC client to the RPC server. There are a total of four packets ir
    a. The RPC Client bind request containing the UUID of the desired RPC Server.
    b. A Write AndX response from the RPC Server
    c. A Read AndX request from the RPC Client.
    d. A Bind ACK response from the RPC Server.
2. At this time a RPC request to the RPC server component is expected.

RPC Communication

At this point RPC communication is occurring between the RPC Client and RPC Server. The troubleshooting steps involved application reporting the RPC failure.

For Active Directory processes or services please see Active Directory Symptoms.

For Microsoft Exchange related RPC errors please see: Analyzing Exchange RPC traffic over TCP/IP

↑ Back to top

How to identify the RPC traffic in a trace

RPC network traffic can take multiple forms. It is important to understand which form is in use in order to identify which TC communication.

RPC over TCPIP

This is sometimes referred to as Traditional RPC or Sockets based RPC. An example of this is Outlook without "Outlook any configured. A TCP session on TCP port 135 is established with the RPC server. To view this traffic in a trace use the filter: "tc the RPC Discovery phase to locate the endpoint of the desired application.

RPC over HTTP

RPC connectivity for Internet connected hosts will typically use RPC over HTTP in order to traverse firewalls. Some example Gateway, Outlook Web Access, Outlook via "Outlook Anywhere". This communication will be established on one or more c 443(SSL). Since this typically traverses a public network, SSL or TCP port 443 is the more common method. Use the filter "tc either form inside network trace.

RPC over HTTP Port 80

For sessions over TCP port 80, the HTTP requests associated with RPC over HTTP will include a UserAgent header that cont version number of the connector.

RPC over HTTP Port 443

Sessions using TCP port 443 will initially establish a TLS session. After this TLS negotiation, the TCP Payload will be encrypte will not be readable in the trace. In this phase, look for failures due to improper certificates, inaccessible Certificate Revoca

For more information on troubleshooting SSL/TLS see:

http://technet.microsoft.com/en-us/library/cc783349(WS.10).aspx

↑ Back to top

RPC over SMB aka “Named Pipes”

RPC can also take advantage of SMB sessions for the purpose of RPC communication. Some examples of this can be seen
Registry service. With the use of RPC over SMB:

1. Establish TCP connection on TCP port 139 or 445.
2. Negotiate dialect request/response
3. SessionSetupANDX request/response. This sequence is used to establish the SMB Session. Authentication occurs du

If a failure in step 1 occurs, see additional troubleshooting steps see: File and Printer Sharing.

Kerberos Authentication

If Kerberos is used, and the client doesn’t currently have a Kerberos ticket for the RPC server, just after the Negotiate Diale
a Kerberos ticket for the Servername/cifs SPN of the RPC server. This exchange will occur over the Kerberos ports TCP or U
Controller. SessionSetupANDX follows and will consist of a single SessionSetupANDX request which includes the Kerberos
Response indicating success or failure of the authentication.

For additional troubleshooting steps during authentication, see Authentication.

NTLM Authentication

If NTLM is used, SessionSetup will result in a SessionSetupANDX response with a status of STATUS_MORE_PROCESSING_RE
challenge. The subsequent SessionSetupANDX Request will include the hashed credentials of the client. At this time, the RI
supplied by the user. To do this, the RPC server will contact a domain controller, and validate the credentials with the netlo
controller. If this is successful, the RPC server will then respond to the client with a SessionSetupANDX Response indicating

For additional troubleshooting steps during authentication, see Authentication.

Troubleshooting Authentication

Verify that authentication is working correctly by checking for Time skew, UDP Fragmentation or an Invalid Kerberos Realm

- Time skew can be verified by running net time /querysntp and net time /setsntp:<PDCe server name>. The /querysn
  specific DC is manually configured as the authoritative time server. The /setsntp:<PDCe server name> switch can be
  the error with the PDC emulator. The PDC emulator is the authoritative time server by default.
- UDP fragmentation can cause replication errors that appear to have a source of RPC server is unavailable. Sympton
  this problem include clients being unable to log on to the domain, administrators being unable join computers to t
  errors with a source of LSASRV and Kerberos errors with an Event ID of 10 in the system log.

  Knowledge base article 244474 - "How to force Kerberos to use TCP instead of UDP in Windows Server 2003, in M
  Windows 2000" provides the steps to resolve this problem.

- An incorrect Kerberos realm can also be at the root of RPC server is unavailable problems. The symptoms that will l incorrect include the following errors when opening AD management tools:

  Naming Convention could not be located because: No authority could be contacted for authentication. Contact you domain is properly configured and is currently online.

  -or-

  Naming information cannot be located because: No authority could be contacted for authentication. Contact your s domain is properly configured and is currently online.

  To verify that the correct Kerberos realm is configured, follow the steps in 837513 - "Domain controller is not func

↑ Back to top

Active Directory Symptoms:

1. If you are experiencing replication problems and getting RPC server is unavailable errors as is reported in repadmin /shc Monitor to determine if RPC traffic is being blocked is the first step when attempting to troubleshoot RPC Server is unavail

[Replications Check,DC2] A recent replication attempt failed:

From DC1 to DC2

Naming Context: CN=Schema,CN=Configuration,DC=xl

The replication generated an error (1722):

The RPC server is unavailable.

The failure occurred at 2003-10-30 11:59.47.

The last success occurred at 2003-10-28 20:50.22.

26 failures have occurred since the last success.

[DC1] DsBind() failed with error 1722,

The RPC server is unavailable..

The source remains down. Please check the machine.

Bermuda\DC1 via RPC objectGuid: 28c78c72-3c95-499a-bcda137a250f069f

Last attempt @ 2003-10-30 11:58.15 failed, result 1722:

The RPC server is unavailable.

Troubleshooting: If IP Security Policies in Active Directory had the Assigned Value to Server (Request Security) set to Yes t article 313190 - "How to use IPSec IP filter lists in Windows 2000" provide details about where to check these settings ar

2. If you are blocking all ICMP traffic between separate AD sites, you will receive the errors below in the output of DCDIAG

Testing server: contoso\DC1

Starting test: Replications

* Replications Check

[Replications Check,DC1] A recent replication attempt failed:

From DC2 to DC1

Naming Context: CN=Schema,CN=Configuration,DC=litware,DC=com

The replication generated an error (1722):

The RPC server is unavailable.

The failure occurred at 2003-08-24 23:00.51.

The last success occurred at (never).

553 failures have occurred since the last success.

[DC2] DsBind() failed with error 1722,

The RPC server is unavailable..

The source remains down. Please check the machine.

REPLICATION LATENCY WARNING

DC1: A full synchronization is in progress

from DC2 to DC1

Replication of new changes along this path will be delayed.

[DC2] LDAP connection failed with error 58,

The specified server cannot perform the requested operation.

Troubleshooting: To resolve this issue, remove the ICMP traffic restriction between domain controllers. When establishing ICMP traffic is used. If the ICMP fails, so does the RPC session establishment, and hence AD replication also fails. ISA 2004 of computers specified in the Remote Management Computers computer set which can be configured in system policy.

3. The following error will appear when attempting to connect to the computer.

"computer <\\servername.domain.local> cannot be managed. The network path was not found. RPC server is unavailable.

Or when viewing the properties of the remote computer you will receive the error:

"Win32: The RPC server is unavailable".

Troubleshooting: Computer management is one of the better tools for testing RPC connectivity. When RPC traffic is being using the computer management console will fail.

4. When attempting to promote an additional domain controller in an Active Directory domain while the RPC service is blo appear:

"The domain "domain.local" is not an Active Directory domain, or an Active Directory domain controller for the domain co

Troubleshooting:

5. Connections to computers via Remote Desktop may fail if RPC connectivity cannot be established. When attempting to the following error will be produced in the form of a popup error message if RPC connectivity is the root of the problem:

"The system cannot log you on due to the following error: The RPC server is unavailable."

You may also see the following errors on the Terminal server:

Error 1727: The remote procedure call failed and did not execute

Error 1722: The RPC server is unavailable.

Error 1723: The RPC server is too busy to complete this operation.

Error 1721: Not enough resources are available to complete this operation.

-or-

Event ID 5719:

Source: NetLogon

Description: No Windows NT Domain Controller is available for domain domain_name.

The following error occurred: There are currently no logon servers available to

service the logon request.

Event ID: 1219

Source: Winlogon

Details: Logon rejected for CONTOSO\<computername>. Unable to obtain Terminal Server

User

Configuration. Error: The RPC server is unavailable.

Troubleshooting: These errors can be a result of the TCP/IP NetBIOS Helper service being disabled on the Terminal server one of the NIC's used to access the Terminal server. You should also verify that the Client for Microsoft networks is bound server. You can tell if this is happening by looking at a Netdiag /v from the box for the following output:

Testing redirector and browser... Failed

NetBT transports test. . . . . : Failed

List of NetBt transports currently configured:

[FATAL] No NetBt transports are configured.

Redir and Browser test . . . . . : Failed

List of transports currently bound to the Redir

NetBIOSSmb

[FATAL] The redir isn't bound to any NetBt transports.

List of transports currently bound to the browser

[FATAL] The browser isn't bound to any NetBt transports.

↑ Back to top

Troubleshooting Tools and Methods

Methods to generate RPC Traffic

Computer Management MMC to a remote host

Outlook to an Exchange server

RPCPing - http://support.microsoft.com/kb/831051

Tools for Testing RPC

RPCPing - http://support.microsoft.com/kb/831051

PortQry - http://support.microsoft.com/default.aspx?scid=kb;EN-US;832919

Pipelist - http://technet.microsoft.com/en-us/sysinternals/dd581625.aspx

RPCDump - http://support.microsoft.com/default.aspx?scid=kb;EN-US;325930

NSLookup - http://support.microsoft.com/default.aspx?scid=kb;EN-US;200525

NBLookup - http://support.microsoft.com/default.aspx?scid=kb;EN-US;830578

Tools for monitoring RPC

Network Monitor - Download – FAQ

Wireshark - Download

Using PortQry

You can use the Portqry tool to verify that the required ports are open. You should run the Portqry tool on a computer that computer that is receiving RPC errors by using the -n switch. To this, follow these steps:

a. Click "Start", click "Run", type "cmd" in the "Open" box, and then click OK".

b. Type "portqry -n <problem_server> -e 135" (without the quotation marks).

The output will appear similar to the following examples:

Querying target system called:

<problem_server>

Attempting to resolve name to IP address...

Name resolved to 169.254.1.1

querying...

<problem_server>

TCP port 135 (epmap service): LISTENING

Using ephemeral source port

Querying Endpoint Mapper Database...

Server's response:

UUID: f5cc59b4-4264-101a-8c59-08002b2f8426 NtFrs Service

ncacn_ip_tcp:65.53.63.16[1094]

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2 MS NT Directory DRS Interface

ncacn_ip_tcp:65.53.63.16[1025]

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2 MS NT Directory DRS Interface

ncacn_http:65.53.63.16[1029]

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2 MS NT Directory DRS Interface

ncacn_http:65.53.63.16[6004]

If port 135 is blocked, the following will appear:

TCP port 135 (epmap service): NOT LISTENING However, for these RPC Endpoint Mapper errors it is likely that ports greate 135.From the output, you know the DC is using port 1094 for FRS and 1025, 1029, and 6004 for Active Directory replicatior check those ports. For example, you can test all the ports at the same time by using the Portqry tool with the -o switch. Fo

"portqry -n <problem_server> -o 1094,1025,1029,6004"(Without the quotation marks)

If the ports all respond as "LISTENING," it's likely that blocked ports are not causing this problem. If any ports respond as " blocked.

↑ Back to top

Resources

RPC Blogs

Basics of RPC are covered here:

RPC to Go v.1: http://blogs.technet.com/b/networking/archive/2008/10/24/rpc-to-go-v-1.aspx

Architecture and a closer look at a connection to the RPC Endpoint mapper in a network capture.

RPC to Go v.2: http://blogs.technet.com/b/networking/archive/2008/12/04/rpc-to-go-v-2.aspx

This describes how RPC commands can be sent over Named Pipes in SMB via the IPC$ Tree.

RPC to Go v.3: http://blogs.technet.com/b/networking/archive/2009/04/28/rpc-to-go-v-3-named-pipes.aspx

Troubleshooting "**RPC server is unavailable**" error, reported in failing **AD replication scenario**.

http://blogs.technet.com/b/abizerh/archive/2009/06/11/troubleshooting-rpc-server-is-unavailable-error-reported-in-failin

External TechNet Magazine article

This one is good. It lays out RPC basics really quickly and then moves on RPC errors. The information on MaxUserPort wo about the dynamic port ranges that are used in Vista/W2008 are the high range of ports compared to the 1025-5000 for V

How IT Works, Troubleshooting RPC Errors by Zubair Alexander:

http://technet.microsoft.com/en-us/magazine/2007.07.howitworks.aspx

KB Article

Troubleshooting RPC Endpoint Mapper errors using the Windows Server 2003 Support Tools from the product CD

https://support.microsoft.com/en-us/help/839880/troubleshooting-rpc-endpoint-mapper-errors-using-the-windows-serve

↑ Back to top
