

Re: ISA Server Error

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2006-08/msg00387.html>

- *From:* Smurfman <smurfman@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 18 Aug 2006 13:31:02 -0700
-

Ken,
Well, it has been an eventful afternoon.

Here is what I have done.

1) Since I am replacing my old Domain Controllers, I noted the solution in KB 898720 where the error "Setup failed while creating the services configuration" this happened during the uninstall, which I finally got to work by disabling all the services for ISA and then rebooting. But it then happened during the install. Since this machine is a DC, this KB resolved the install issue.

2) Replication is still having some trouble. I noted that I could not get the logging to work so that I could see what I was attempting to make work RPC, LDAP etc etc, the things getting blocked that seem to be needed.

3) The new issue was that I could not make firewall rule changes, even though I had full ISA admin rights per the delegation. I was getting this error "The configuration changes were saved to storage, but at least one service failed to load these changes. The event viewer may...". And logging would not work, since I would get this error, "The Query stopped because an error occurred while it was running." I found KB 914957, and called for the hotfix (BTW the script has a typo in it, I had to fix the hotfix suggestion.) This replaced the w3filter.dll and the wpsrv.exe from version 4.0.2165.594 to 4.0.2165.601, this did nothing, still have the same error.

4) Searched google for a while, found this link...

http://www.experts-exchange.com/Operating_Systems/Windows_Server_2003/Q_21384303.html

The solution for this person was to change the Microsoft Firewall service from NETWORK SERVICE to Local Server for the logon.

I did this (step 4) restarted Microsoft Firewall and "poof" everything was working.

SO...

A) What did I just break?

Re: ISA Server Error

- B) What security hole did I just create?
- C) Where was the NETWORK SERVICE attempting to go, that it could not?
- D) Where is the storage that the Firewall Rules error was referring to that could not load the changes?

Thanks
J

""Ken Zhao [MSFT]"" wrote:

Hello,

Thank you for using newsgroup!

Based on my knowledge, this error message may occur if the permission for the following registry key is incorrect:

HKEY_LOCAL_MACHINE\Software\Microsoft\Fpc\Arrays\<GUID>\SingaledAlerts

The default permission should be
Administrators: Full Control
SYSTEM: Full Control

You may open regedt32, then from the tool bar, select Security and Permissions. You can manually add the permission, or check the box "Allow inheritable permissions from parent to propagate to this object". This should inherit the same permission (Administrators: Full Control, SYSTEM: Full Control) from HKEY_LOCAL_MACHINE\Software\Microsoft\Fpc

Hope that helps!

Thanks & Regards,

Ken Zhao

Microsoft Online Partner Support
Get Secure! – www.microsoft.com/security

=====
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.
=====

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

Re: ISA Server Error

| Thread-Topic: ISA Server Error
| thread-index: AcbCCF40fsudIMh9Ste/exulJ9iYjA==
| X-WBNR-Posting-Host: 209.217.222.70
| From: =?Utf-8?B?U211cmZtYW4=? <smurfman@xxxxxxxxxxxxxxxx>
| References: <32ABAAAB-CF8B-41B3-867F-91164376747B@xxxxxxxxxxxxxxxx>
<ubcsBSgwGHA.428@xxxxxxxxxxxxxxxxxxxxxxxx>
| Subject: Re: ISA Server Error
| Date: Thu, 17 Aug 2006 07:21:02 -0700
| Lines: 223
| Message-ID: <85493246-6029-42AA-B0EE-98316D719A82@xxxxxxxxxxxxxxxx>
| MIME-Version: 1.0
| Content-Type: text/plain;
| charset="Utf-8"
| Content-Transfer-Encoding: 8bit
| X-Newsreader: Microsoft CDO for Windows 2000
| Content-Class: urn:content-classes:message
| Importance: normal
| Priority: normal
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.1830
| Newsgroups: microsoft.public.isa
| Path: TK2MSFTNGXA01.phx.gbl
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.isa:67646
| NNTP-Posting-Host: TK2MSFTNGXA01.phx.gbl 10.40.2.250
| X-Tomcat-NG: microsoft.public.isa

| Thanks Shijaz,
| I think I did this, in fact I reviewed the rights, I added the specific
user
| name, and also the domain/domain admins, to have full isa rights...

| Oh, also the BUILTIN/Administrators

| My gut tells me there is something whacky with dns...

| J

| "Shijaz" wrote:

| >>I am getting this error anytime that I attempt to view the dashboard
or

| >>make

| >> a change in ISA 2004...

| >>

| >> "Refresh Failed"

| >> "You do not have the necessary permissions to perform this action."

| >>

| >> Yet the user is a domain admin that is logged into the machine...I
can't

| >> even monitor the logs, make a rule change or anything.

| >

Re: ISA Server Error

|> Make sure you delegated permissions to this user from the ISA console while

|> you were logged in as the original administrator. To delegate permissions,

|> under "Configuration", choose "General". You will find the option to delegate in the middle pane.

|>

|> Shijaz Abdulla

|> MCSE:Security, CCNA

|> www.shijaz.com/isaserver

|>

|>

|>

|>

|>

|> "Smurfman" <smurfman@xxxxxxxxxxxxxxxx> wrote in message

|> news:32ABAAAB-CF8B-41B3-867F-91164376747B@xxxxxxxxxxxxxxxx

|>>I am getting this error anytime that I attempt to view the dashboard

or

|>>make

|>> a change in ISA 2004...

|>>

|>> "Refresh Failed"

|>> "You do not have the necessary permissions to perform this action."

|>>

|>> Yet the user is a domain admin that is logged into the machine...I can't

|>> even monitor the logs, make a rule change or anything.

|>>I am getting this error anytime that I attempt to view the dashboard

or

|>>make

|>> a change in ISA 2004...

|>>

|>> "Refresh Failed"

|>> "You do not have the necessary permissions to perform this action."

|>>

|>> Yet the user is a domain admin that is logged into the machine...I can't

|>> even monitor the logs, make a rule change or anything.

|>>

|>>

|>> I have these entries in the Event log, and I have a feeling that I have

|>> configured something in the firewall that is not allowing my server to get

|>> authenticated or synchronized with my other servers.

|>>

|>> (To understand what I am attempting is that I have built two new machines

|>> to

|>> eventually replace two older machines. DC_1 is an old W2K Domain

Re: ISA Server Error

|>> Controller,
|>> and is being replaced with DC_2 a new W2K3 R2 server. I have already
|>> built
|>> this machine, made it a DC in the forest, installed DNS (AD
integrated),
|>> but
|>> have not moved the Global Catalog, or demoted the old server or moved
any
|>> of
|>> the roles to the new DC_2. This new server seems to be replicating
just
|>> fine
|>> with the others....
|>>
|>> ISA_1 is also being replaced (ISA2000 on W2K) with a new W2K3 R2
server
|>> with
|>> ISA 2004 (ISA_2). In my model the old ISA_1 server served as a
backup DC
|>> and
|>> in our small network this has worked just fine for the past 5 years.
|>> Having
|>> said that, I converted my new ISA_2 server to a DC, but noted that
|>> replication was not working properly, the ISA logs were showing deny
|>> entries
|>> for "RPC (all interfaces)" dropping on my all access rule, that was
|>> specific
|>> to Administrators and the local System and Network groups.
Administrators
|>> was a group I defined as my DOMAIN\Domain Admins built in account,
and a
|>> couple of other specific users. Using the Sonar tool to monitor
|>> replication,
|>> the servers were finally talking but I am getting an error with the
Sonar
|>> tool – DataCollectionState failed with a DataCollectionError of SCM.
I do
|>> not know what this is telling me.)
|>>
|>> My ISA_2 server is pointing to my new DC_2 server for DNS
|>>
|>> From the ISA_2 server, running AD Sites and Services, I note that the
new
|>> DC_2 server has 3 NTDS entries (connections to the other 3 DC's), my
old
|>> DC_1
|>> server only has 2 NTDS connections (1 to ISA_1 and 1 to DC_2). My
ISA_2
|>> server only has 2 connections (1 to DC_2 and 1 to ISA_1), and finally
|>> ISA_1
|>> has 3 connections (1 to ISA_2, 1 to DC_1, and 1 to DC_2).

Re: ISA Server Error

|>>
|>> While the connection is present, an attempt to replicate to ISA_2
from
|>> ISA_1
|>> results in this error:
|>>
|>> "The following error occurred during the attempt to synchronize naming
|>> context DOMAINNAME.com from domain controller ISA_2 to domain
controller
|>> ISA_1: The RPC server is unavailable."
|>>
|>> "This operation will not continue. This condition may be caused by a
DNS
|>> lookup problem. For information about troubleshooting common DNS
lookup
|>> problems, please see the following Microsoft Web Site:
|>> <http://go.microsoft.com/fwlink/?LinkId=5171>
|>>
|>> I know this is a long post, but the more info I suppose the better.
Much
|>> appreciated.
|>>
|>> J
|>>
|>> Other errors in the event logs are like such...
|>>
|>> Event Type: Error
|>> Event Source: Userenv
|>> Event Category: None
|>> Event ID: 1030
|>> Date: 8/17/2006
|>> Time: 9:08:41 AM
|>> User: NT AUTHORITY\SYSTEM
|>> Computer: ISA_2
|>> Description:
|>> Windows cannot query for the list of Group Policy objects. Check the
event
|>> log for possible messages previously logged by the policy engine that
|>> describes the reason for this.
|>>
|>> For more information, see Help and Support Center at
|>> <http://go.microsoft.com/fwlink/events.asp>.
|>>
|>> Event Type: Error
|>> Event Source: Microsoft Firewall
|>> Event Category: None
|>> Event ID: 21137
|>> Date: 8/17/2006
|>> Time: 8:53:08 AM
|>> User: N/A
|>> Computer: ISA_2

Re: ISA Server Error

|>> Description:
|>> The connectivity verifier "DNS" reported an error when trying to connect
|>> to
|>> DC 2.DOMAINNAME.com.
|>> Reason: The request has timed out.
|>>
|>> For more information, see Help and Support Center at
|>> <http://go.microsoft.com/fwlink/events.asp>.
|>>
|>> Event Type: Warning
|>> Event Source: LSASRV
|>> Event Category: SPNEGO (Negotiator)
|>> Event ID: 40960
|>> Date: 8/16/2006
|>> Time: 4:17:21 PM
|>> User: N/A
|>> Computer: ISA_2
|>> Description:
|>> The Security System detected an authentication error for the server
|>> ldap/isa_2.DOMAINNAME.COM. The failure code from authentication
protocol
|>> Kerberos was "There are currently no logon servers available to
service
|>> the
|>> logon request.
|>> (0xc000005e)".
|>>
|>> For more information, see Help and Support Center at
|>> <http://go.microsoft.com/fwlink/events.asp>.
|>> Data:
|>> 0000: 5e 00 00 c0 ^..Ã€
|>>
|>> Event Type: Warning
|>> Event Source: DnsApi
|>> Event Category: None
|>> Event ID: 11164
|>> Date: 8/16/2006
|>> Time: 4:17:35 PM
|>> User: N/A
|>> Computer: ISA_2
|>> Description:
|>> The system failed to register host (A) resource records (RRs) for
network
|>> adapter
|>> with settings:
|>>
|>> Adapter Name : {706E8886-34B6-45E5-B9BB-BB957122E48F}
|>> Host Name : isa_2
|>> Primary Domain Suffix : DOMAINNAME.COM
|>> DNS server list :

Re: ISA Server Error

|>> 192.168.1.19

|>> Sent update to server : <?>

|>> IP Address(es) :

|>> 192.168.1.18

|>>

|>> The reason the system could not register these RRs was because either

(a)