

Re: Windows firewall in 2 node 2K3 Cluster

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.clustering/2006-03/msg00036.html>

- *From:* Scott Dungan <ScottDungan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 2 Mar 2006 12:15:27 -0800
-

Thanks for the reply Ryan. Here is what I did and what I found:

I did set the HB network for only Private and the public network as Public only. I also made sure the "Network Priority" had only the HB network listed.

This seemed to resolve the issue while both nodes were running. Once I initiated a test failover by stopping the cluster service on node2 I ran into problems. Node1 took over the cluster resource as it should and I was still able to access the virtual server from a client. Looking good so far...

But, When I went to node2 and attempted to bring it back online with cluster administrator, cluster admin gave me a "RPC server is unavailable" error when attempting to connect to the virtual server. I noticed that there was a bunch of activity on the private nic on node2 while it was attempting to connect to the virtual server, but then it times out and gives the RPC error.

I also noticed that it is using the FQDN of the virtual server when it reports the error. If it is attempting to contact the cluster/virtual server using that name, the name resolution will point it to the public address and not the private one, thus hitting the firewall.

To test this I dropped the firewall on the active node (node1) and the cluster admin console on node2 came up just fine and I was able to bring node2 back on line.

Further testing showed that enabling the firewall on either node whilst it was the active node, cause the passive node to be unable to contact the virtual server through cluster admin.

So it would seem that cluster admin still uses the public net to contact the virtual server for administration purposes. Perhaps an entry in the hosts files of the nodes to point the virtual server name to the private IP of each node?

"Ryan Sokolowski (MVP)" wrote:

Re: Windows firewall in 2 node 2K3 Cluster

The way to force all the internal cluster communications traffic to the HB network is...

Make sure that in your networks configurations, you have the private or HeartBeat network listed as Private only and you have the Public network listed as Public only. Also check the following...

Right-Click on the Cluster Object and select "Properties"
Select the "Network Priority" tab
Make sure the HeartBeat network is the only one listed

--
--

Ryan Sokolowski
MVP – Windows Server – Clustering
MCSE, CCNA, CCDA, BCFP

"A troubleshooter's best tool is the Event Viewer and understanding the events and messages contained therein."

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

"Scott Dungan" <Scott Dungan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:D1B8E940-1682-4CCF-90C9-287FED18C078@xxxxxxxxxxxxxxxxxxxx

Hello. I have a 2 node cluster that I want to secure using Windows Firewall.
Specifically, I want to only firewall the public interfaces, as the private network for heartbeat and other cluster communication is only accessible to the cluster nodes.

When I attempt to do this (even with the File and Print Sharing exception enabled) I receive "RPC service unavailable" errors when attempting to add the second node to the cluster. As soon as I drop the firewalls on the public interfaces, everything works fine.

I understand from a few MS KBs (see link below) that there are a range of dynamic ports that need to be open for MSCS to function correctly. My question is this: Is there a way to force all of this traffic to the private, un-firewalled network? If not, is there a way to force this RPC traffic on a single port or just a few?

Re: Windows firewall in 2 node 2K3 Cluster

Any help would be much appreciated!

<http://technet2.microsoft.com/WindowsServer/en/Library/252262df-acd5-484d-b7b3-80ffe0d9d1b2>