Windows Insider

35,000 Subscribers Worldwide

April 17, 2002
Issue #88

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

CramSession

Feature

Adventures with Windows Network Load Balancing and ISA

to top

Server

Windows 2000 Advanced Server includes just a few services worth having that you can't get with Windows 2000 Pro or Server. One of those services is the Windows Network Load Balancing Service (NLB). NLB allows you to provide load balancing and fault tolerance for your servers by allowing two or more NLB cluster servers to share a single IP address. Messages sent to the NLB address are automatically load-balanced based on how you configure NLB. If one or more of the servers in the NLB cluster goes down, the remaining servers will be able to take over the duties of the downed machines. Very cool.

NLB is a virtual no-brainer when working with single-homed machines, but can be a bit of a challenge when you're working with multihomed machines such as firewalls. I've been spending a lot of time recently working with ISA Server and NLB, and it's been an interesting experience. The good news is that you can get NLB to work with ISA Server. The bad news is there are some "gotcha's" along the way to making it work.

Configuring ISA Servers in an NLB array allows you to increase the fault tolerance of your ISA Server solution. If you are primarily concerned with outbound access, you can ensure that your internal network clients will be able to access the Internet by configuring two or more ISA Servers in an NLB cluster by adding NLB to the internal interface of the ISA Servers. If you are more concerned with making sure that servers on your internal network are always accessible to external network users, you can add NLB to the external interface of the ISA Servers.

Yes, it's an either/or thing with the Windows 2000 NLB. In a dual-homed ISA Server, NLB can only be configured on one of the interfaces. That's why you have to choose whether to configure NLB for inbound or outbound access. If you want NLB fault tolerance for your internal and external network clients, you'll have to configure two arrays; one for inbound access and one for outbound.

NLB works without a hitch when you configure the ISA Servers to use it on their internal interfaces. You configure all the ISA Servers in the NLB array to use the same virtual IP address on the internal interface. After all the members of the array have converged (i.e., all the array members of detected one another), you're ready to rock. The only thing left to do is configure the internal network clients to route Internet bound requests to the virtual IP address bound to the internal interface of the ISA Servers.

Things work a bit differently when you want to configure the external interfaces of the ISA Servers to participate in an NLB array. Why would you configure the internal interfaces of the ISA Servers to be members of an NLB array? The primary reason is to provide fault tolerance for your server publishing solution. If you want to make servers on the internal network available to Internet users, you use ISA Server Publishing Rules. The external network users connect to the virtual IP address on the external interface of the ISA Server array. If one of the servers goes down, no problem! External network users will still be able to access the internal network resources through one of the remaining ISA Servers in the array.

The problem with NLB on the external interface of the ISA Servers isn't with NLB itself, its how the ISA Server NAT engine handles the packets that are passed to the internal network servers. By default, when an ISA Server receives a packet from an Internet user that is destined to a published server on the internal network, the packet it passed to the internal network server still contains the ORIGINAL IP address of the Internet host in the source IP address field.

This normally isn't a problem, because the internal network server is configured with a default gateway that it uses to respond to the request made from the Internet host. However, we do have a problem because if the server on the internal network uses a default gateway that is not the same machine that passed the packet from the Internet host to the internal network server, the response will be dropped. The reason for this is that session state information is not shared among NLB array members. If the internal network server's response is sent to an ISA Server in the NLB array that did not originally handle the packet, that ISA Server drops it because it doesn't know anything about it!

The internal network server responding to the Internet host's request has no knowledge of the ISA Server NLB array member that passed the packet. All the publishing server knows is that the source address is a remote network, and therefore it needs to forward its response to its default gateway address for appropriate routing. If you have 4 ISA Servers in your NLB array, there's only a 25% chance that the gateway for the reply will be the same machine that passed the inbound packet to the published server.

There is a solution to this problem. If you install ISA Server Service Pack 1, and then configure the registry entry noted in Q311777, the source address of the packet passed to the internal network server is changed. Instead of the source IP address being the IP address of the Internet host that sent the request, the source address is the IP address of the internal interface of the ISA Server than handled the packet. Now the publishing server doesn't need to use a gateway to route to the Internet, because the response is sent to the internal interface of the ISA Server that handled that packet, and that interface address is on the internal network (and therefore the internal server doesn't require a route to the Internet).

This is pretty cool! But there are two problems. First, the source IP address in your server logs will always be an address on one of the ISA Server array members. If you need the original source IP address for accounting purposes, too bad! Well, you could monkey around with parsing the Firewall service logs, but most automated routines work on the server logs, not the firewall logs. Second, if the publishing server also needs fault tolerance for outbound access (servers that initiate new connections, not just responses), enabling NLB on the external interface does them no good at all.

There are solutions to this problem, but neither of them comes with Windows 2000 Advanced Server right out of the box. One is to use a software add-on, such as Stonesoft's StoneBeat Full Cluster software. This is a very nice package that plugs into ISA Server flawlessly, and allows bi-directional NLB array configuration. Another option is to wait for .NET Server to come out. .NET Advanced Server will support bi-directional NLB for ISA Server. Needless to say, I can't wait!

NLB is a really cool tool that provides functionality that you would have to pay thousands of dollars for if you were to use a third-party hardware fault tolerance and load balancing solution. NLB also improves your overall security scheme because it improves your uptime. I'll be writing more about NLB in the future, because there are a lot of ways you can use this tool to make your live better and easier.

This week's feature article by
Thomas W. Shinder,
M.D., MCSE

Ask Uncle Bill

Q and A's

to top

Question:

Hi, Uncle Bill.
I have a DC and another two computers are the child DCs of the existing DC . If the main DC fails, please give me the steps to activate
--sajeev s

Uncle Bill says:

Yo Sajeev! Windows 2000 Domain Controllers are all equal partners in crime. Unlike the Windows NT 4.0 PDC/BDC arrangement, you don't have a hierarchy of domain controllers. However, like Napoleon the Pig would say "some pigs are more equal than others". This refers to Windows 2000 FSMO roles. If the DC that went down is the only Global Catalog server, you'll need to make one of the other DCs a Global Catalog server, since without an online GC, no one will be able to log onto the domain. If you don't intend on bringing the downed DC up again, then you can have one of the other DCs seize the other FSMO roles, but you not do this if the dead DC plans to see the light of day again. Check out the Windows 2000 Help file on how to configure a DC to be a GC Server and how to seize FSMO roles.

Question:

Hi, Uncle Bill
Did you read Shinder's article last week? I think that guy is a real dope! He said that DNS has nothing to do with port numbers. How about TCP/UDP Port 53? And did that guy even read his own book? What about _q931 records required by H.323 Gatekeepers to resolve domain names for email addresses? You have to enter the TCP port number in the SRV record! Tell him to take his Ginko and Geritol when you see him; maybe that will stimulate his flagging brain cells.
-–Young Turk

Uncle Bill says:

Listen, YT. I talked to Shinder about this and he said he was talking about traditional Host (A) records, not those fancy SRV record things. But you're right. SRV records allow you to specify port information for services and Shindork should have said something about this. The DNS Query and Zone Transfer ports are another issue. While you need to take these ports into account when configuring access through firewalls and such, they are defined by the DNS protocol, and aren't something you consider when creating Host records. But he should have made a note of this too, just to be complete. I'll make sure to whip the dude with the cat o' nine tails the next time he walks past my cell.

Don't Be Shy!

Got a question about MCSE certification or an event log error that just won't go away? Send it in! We'll be answering a question or two every week. Send your submissions to Uncle Bill **here**.

Security Advisories

Cumulative Patch for Internet Information Services

▲ to top

This patch is a cumulative patch that includes the functionality of all security patches released for IIS 4.0 since Windows NT 4.0 Service Pack 6a, and all security patches released to date for IIS 5.0 and 5.1. Be sure to read all the information on the patch site to see if the fix breaks anything you need. Be sure to always test these patches on a non-critical system before deploying them.

Read more...

Unchecked Buffer in Internet Explorer and Office for Mac Can Cause Code to Execute

▲ to top

Got a Mac lying around the house or office? If so, then you need to update your Internet Explorer. This is a fix for a buffer overflow issue with IE and Office for the Mac.

Read more...

News Headlines and Resources

Getting a Good Foundation

▲ to top

The Tech Boom caused many a young networking novitiate to put the cart before the horse. They were trying to get an MCSE before having a thorough understanding of general computer and networking principles. Do you have a good foundation? Check out this article by Mary Robinson and decide for yourself.

Read more...

The Universal Hard Drive Kicks!

▲ to top

Are you tired of copying files to floppies or wimpy little CD-ROMs? Are you a road warrior who needs to copy lots of files and have them immediately available to you wherever you go? Then try out the Universal SmartDrive. It fits on a keychain and you can one that fits up to a Gig of data.

Read more...

The Future of Microsoft Office: Crippleware

▲ to top

Word is out that the future of Microsoft Office is pretty bleak. Just to speed its demise, Microsoft is considering converting the venerable old Office suite into a Crippleware/ Rentware Frankenstein hybrid. You'll be able to rent it out for a year before it explodes on your desktop.

Read more...

Microsoft Baseline Security Analyzer Ready for Prime Time

to top

Microsoft just released a very cool tool that you can use to scan a single computer or a number of computers on your network. This tool is a nicely done GUI front-end for the HFNetChk tool. Check it out!

Read more...

Microsoft Releases Command Line Port Scanner

to top

Here's another port scanner you can add to your toolkit. No frills, but it gets the job done, and it's easily scriptable, so you can use it to monitor the health of your servers and services.

Read more...

Assigning Scripts using Group Policy in Windows 2000

to top

Need a reason to implement Active Directory? How about the ability to assign scripts via Group Policy? Assign scripts by user, OU, or an entire domain. Scripts can be assigned at log on or log off. For details, check out Dan Dinicolo's article here.

Read more...

How to Configure Exchange to Forward Mail to an External Address

to top

Email forwarding is a handy feature that allows you to forward mail from one account to another. Often users want to forward mail sent to their Exchange mailbox to a Web mail service such as Hotmail while they're on the road. This article takes you through the steps to make it happen.

Read more...

Setting Up the ISA Server Message Screener to Support Bidirectional Traffic

to top

One of the cool toys that comes with ISA Server is the SMTP Message Screener. This feature allows you to screen out mail messages that contain certain attachments or keywords in the subject line or body of the message. This article describes how you can get it to screen incoming AND outgoing messages.

Read more...

Support WebCast - Microsoft Exchange 2000 Server: DNS Troubleshooting in Transports

to top

During this Support WebCast, they will focus on how to troubleshoot mail flow problems in Exchange 2000 due to DNS. They will cover configurations for both Exchange 2000 and the DNS servers. Other topics will include symptoms, verification, and some internal concepts in Exchange 2000.

Read more...

Download of the Week

VMware 3.1

to top

I pity the fool who installs hotfixes and new network services without fully testing them in a lab setting first. What? You company doesn't provide you with 5-10 computers to use for a test network? No problem! Check out VMware's latest release, version 3.1, and create that test network on a single machine. This version supports Windows .NET Server, has improved USB support, and lots more!

Read more...

CramSession
Prepare for Success!

Your subscribed e-mail address is:steven.thode@toadworld.net
To unsubscribe, simply **click here** and hit "send" in your e-mail reader,
or visit the **CramSession Unsubscribe Page** .