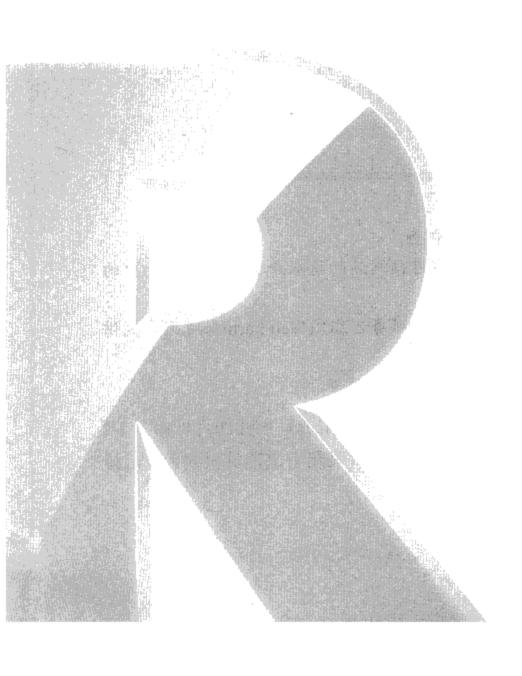
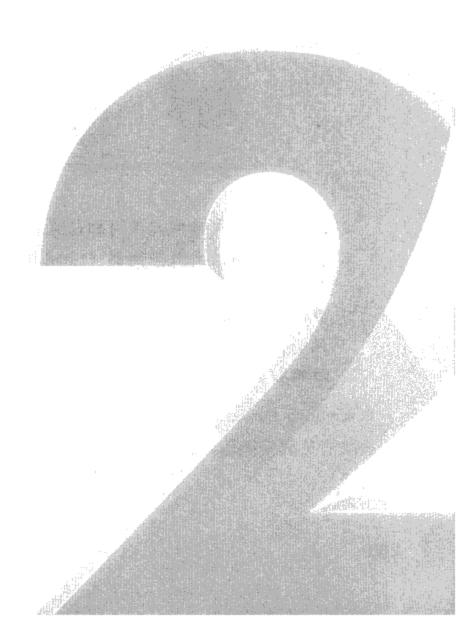
第章

Web Farm与网络负载平衡(NLB)

通过将多台IIS Web服务器组成Web Farm的方式,可以提供一个具备排错与负载平衡的高可用性网站。本章将详细分析Web Farm与Windows网络负载平衡(Windows Network Load Balancing,简称Windows NLB或WNLB)。

- > Web Farm与网络负载平衡概述
- > Windows系统的网络负载平衡概述
- ≥ IIS网页服务器的Web Farm实例演练
- ≥ Windows NLB群集的高级管理





7-1 Web Farm与网络负载平衡概述

将企业内部多台IIS Web服务器组成Web Farm后,这些服务器将同时对用户来提供一个不间断的、可靠的网站服务。当Web Farm接收到不同用户的连接网站请求时,这些请求会被分散地送给Web Farm中不同Web服务器来处理,因此可以提高网页访问效率。若Web Farm之中有Web服务器因故无法对用户提供服务的话,此时会由其他仍然正常运行的服务器来继续对用户提供服务,因此Web Farm还具备排错功能。

7-1-1 Web Farm的架构

图 7-1为一般Web Farm架构的示例,图中为了避免单点故障而影响到Web Farm的正常运行,因此每一个关卡,例如防火墙、负载平衡器、IISWeb服务器与数据库服务器等都不只一台,以便提供排错、负载平衡功能:

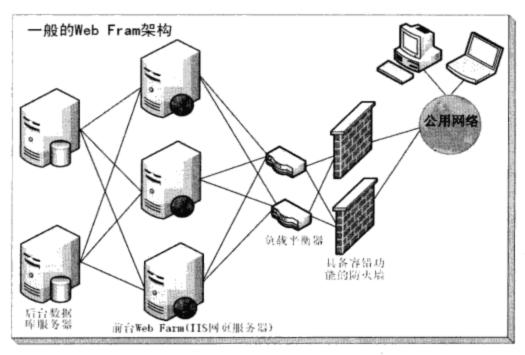


图 7-1

- ▶ 防火墙: 防火墙可确保内部计算机与服务器的安全。
- 负载平衡器: 负载平衡器 (Load Balancer) 可将连接网站的请求分发到Web Farm中的不同Web服务器。
- **前端Web Farm (IIS Web服务器)**: 将多台IIS Web服务器组成Web Farm来对用户提供 网页访问服务。
- 后端数据库服务器: 用来存储网站的设置、网页或其他数据。

Windows Server 2008 R2已经内置网络负载平衡功能(Windows NLB), 因此您可以如图 7-2 所示取消负载平衡器,改在前端Web Farm启用Windows NLB,并利用它来提供负载平衡与排错功能。

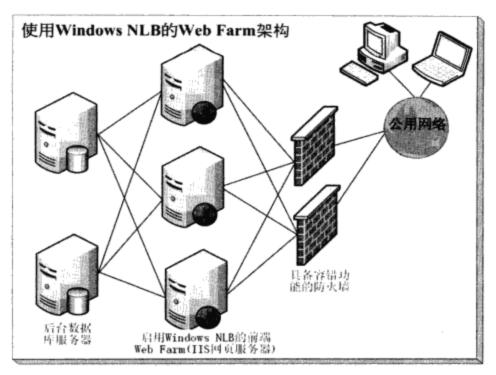


图 7-2

还有因为Microsoft ISA Server或Microsoft Forefront Threat Management Gateway(TMG)的 防火墙可以通过发行规则来支持Web Farm,因此可以如图 7-3所示来搭建Web Farm环境。

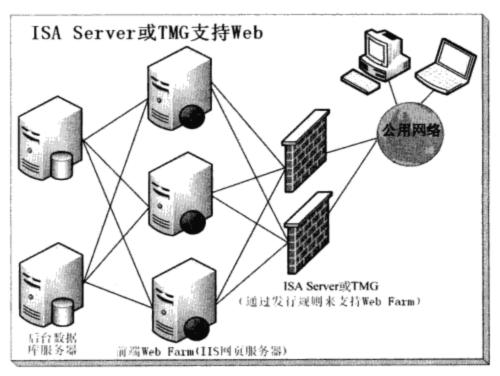


图 7-3

图中ISA Server或TMG接收到外部连接内部网站请求时,它会根据发行规则的设置,来将此请求转发交给Web Farm中的一台Web服务器处理。ISA Server或TMG也具备自动检测Web服务器是否停止服务的功能,因此它只会将请求转发给仍然正常运行的Web服务器。

7-1-2 网页内容的存储地点

您可以如图 7-4所示将网页存储在每一台Web服务器的本地磁盘内(图中我们将防火墙与 负载平衡器各简化为一台), 您必须让每一台Web服务器内所存储的网页内容都相同, 虽然可

以利用手动复制的方式来将网页文件复制到每一台Web服务器,不过建议采用DFS(分布式文 件系统)来自动复制,此时只要更新其中一台Web服务器的网页文件,它们就会通过DFS复制 功能自动复制到其他Web服务器。

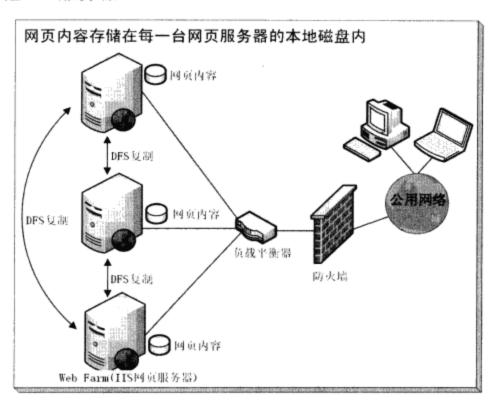


图 7-4

您也可以如图 7-5所示将网页存储到SAN(Storage Area Network)或NAS(Network Attached Storage)等存储设备内,并利用它们来提供网页内容的排错功能。

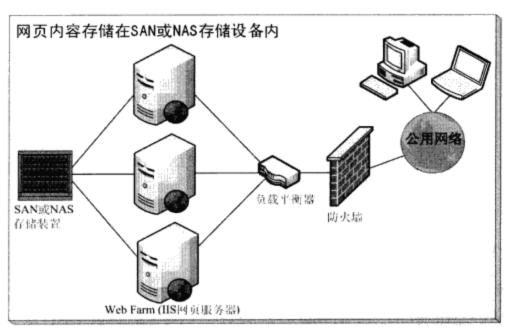


图 7-5

您也可以如图 7-6所示将网页存储到文件服务器内,而为了提供排错功能,因此应该架设 多台文件服务器,同时还必须确保所有服务器内的网页内容都相同,您可以利用DFS复制功能 来自动让每一台文件服务器内所存储的网页内容都相同。

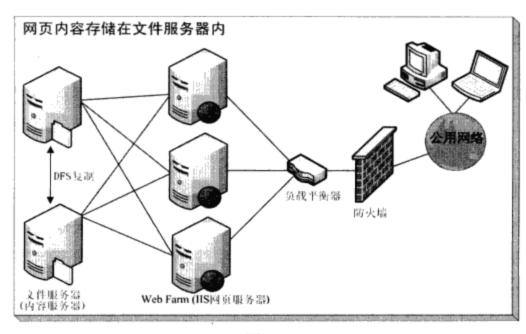


图 7-6

7-2 Windows系统的网络负载平衡概述

由于Windows Server 2008 R2系统已经内置了网络负载平衡功能(Windows NLB),因此我们可以直接采用Windows NLB来搭建Web Farm环境。例如图 7-7中Web Farm内每一台Web服务器的外网卡各有一个**固定IP地址**,这些服务器对外的流量是通过固定IP地址送出。而在您创建了NLB群集(NLB cluster)、启用外网卡的Windows NLB、将Web服务器加入NLB群集后,它们还会共享一个相同的**群集IP地址**(又称为**虚拟IP地址**),并通过此群集IP地址来接收外部的上网请求,NLB群集接收到这些请求后,会将它们分散地交给群集中的Web服务器来处理,因此可以达到负载平衡的目的,提高运行效率。

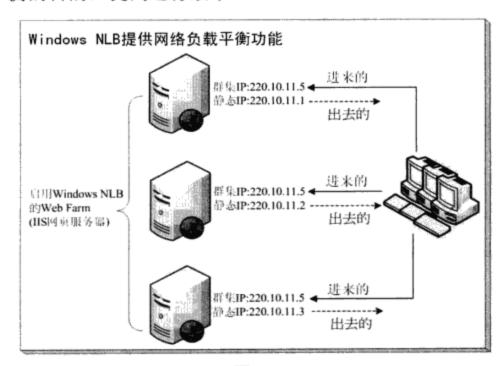


图 7-7

7-2-1 Windows NLB的排错功能

若Windows NLB群集内的服务器成员有异动的话,例如服务器故障、服务器脱离群集或 增加新服务器,此时NLB会启动一个称为聚合(convergence)的程序,以便让NLB群集内的 所有服务器拥有一致的状态并重新分配工作负担。

举例来说,NLB群集中的服务器会随时监听其他服务器的心跳(heartbeat)状况,以便检 测是否有其他服务器故障,若有服务器故障的话,检测到此状况的服务器便会启动**聚合**程序。 在**聚合**程序执行当中,现有正常的服务器仍然会继续服务,同时正在处理中的请求也不会受 到影响,当完成**聚合**程序后,所有连接Web Farm网站的请求,会重新分配给剩下仍正常的Web 服务器来负责。例如图 7-8中最上方的服务器故障后,所有由外部来的连接Web Farm网站的请 求,会重新分配给其他两台仍然正常运行的Web服务器来负责。

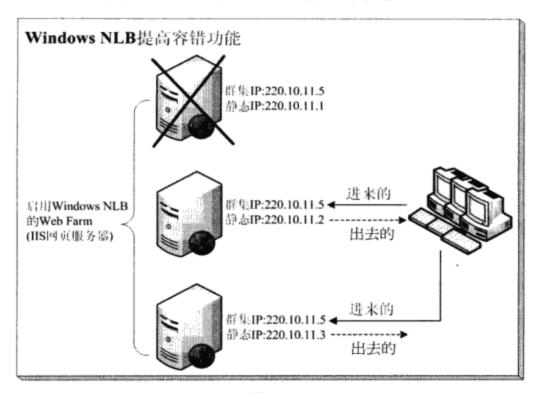


图 7-8

7-2-2 Windows NLB的相似性

相似性 (affinity) 用来定义源主机与NLB群集成员之间的关系。举例来说,如果群集中有 3台Web服务器, 当外部主机(源主机)要连接Web Farm时,此请求是由Web Farm中的哪一台 服务器来负责处理呢? 它是根据Windows NLB所提供的3种相似性来决定的:

➤ 无 (None): 此时NLB是根据源主机的IP地址与端口,来将请求指派给其中一台服务 器处理。群集中每一台服务器都有一个**主机ID** (host ID),而NLB根据源主机的IP地址 与端口所算出来的哈希值(hash)与主机ID有着关联性,因此NLB群集会根据哈希值, 来将此请求转交给拥有相对主机ID的服务器来负责。

因为是同时参照源主机的IP地址与端口,因此同一台外部主机所提出的多个连接Web

Farm请求 (源主机的IP地址相同、TCP端口不同),可能会分别由不同的Web服务器来负责。

- ▶ 单一 (Single): 此时NLB仅根据源主机的IP地址,来将请求指派给其中一台Web服务器处理,因此同一台外部主机所提出的所有连接Web Farm要求,都会由同一台服务器来负责。
- **网络**(Network): 它是根据源主机的C类网络地址(IP地址中最高3个字节),来将请求指派给其中一台Web服务器处理。也就是IP地址中最高3个字节相同的所有外部主机,其所提出的连接Web Farm请求,都会由同一台Web服务器负责,例如IP地址为201.11.22.1 到201.11.22.254(它们的最高3个字节都是201.11.22)的外部主机的请求,都会由同一台Web服务器来负责。

虽然Windows NLB默认是通过相似性来将客户端的请求指派给其中一台服务器来负责,但我们可以另外通过端口规则(port rule)来改变相似性,例如可以在端口规则内将特定流量指定由优先级较高的一台服务器来负责处理(此时该流量将不再具备负载平衡功能)。系统默认的端口规则是包含所有流量(所有端口),且会按照所设置的相似性来将客户端的请求指派给某台服务器来负责,也就是所有流量都具备着网络负载平衡与排错功能。

7-2-3 Windows NLB的操作模式

Windows NLB的操作模式分为单播模式与多播模式两种。

单播模式 (unicast mode)

此种模式之下,NLB群集内每一台Web服务器的网卡的MAC地址 (物理地址)都会被替换成一个相同的**群集MAC地址**,它们通过此群集MAC地址来接收外部来的连接Web Farm请求,传送到此群集MAC地址的请求,会被送到群集中的每一台Web服务器。不过采用单播模式的话,会遇到一些问题,以下列出这些问题所在与解决方案。

⇒ 二层交换机的每一个port所注册的MAC地址必须唯一

如图 7-9所示两台服务器连接到二层交换机(Layer 2 Switch)的两个port上,这两台服务器的MAC地址都被改为相同的群集MAC地址02-BF-11-22-33-44,当这两台服务器的数据包传送到交换机时,交换机应该将它们的MAC地址注册到所连接的port上,然而这两个数据包内的MAC地址都是相同的02-BF-11-22-33-44,而交换机的每一个port所注册的MAC地址必须是唯一的,也就是不允许两个port注册相同的MAC地址。

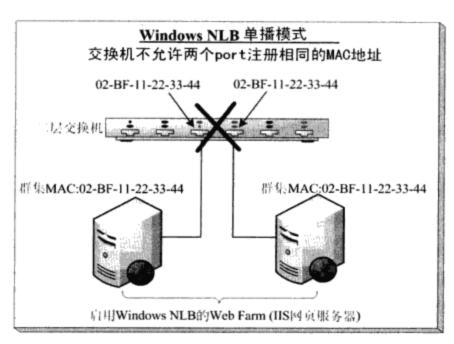


图 7-9

Windows NLB利用MaskSourceMAC功能来解决这个问题,它会根据每一台服务器的主机 ID (host ID) 来更改外送数据包的Ethernet header中的源MAC地址,也就是将群集MAC地址中 最高第2组字符改为**主机ID**,然后将此修改过的MAC地址当作是源MAC地址。

例如图 7-10中的群集MAC地址为02-BF-11-22-33-44,而第1台服务器的**主机ID**为01,则其 外送数据包中的源MAC地址会被改为02-01-11-22-33-44,因此当交换机收到此数据包后,其相 对应的port所注册的MAC地址是02-01-11-22-33-44; 同理第2台服务器所注册的MAC地址为 02-02-11-22-33-44, 如此就不会有两个port注册相同MAC地址的问题。

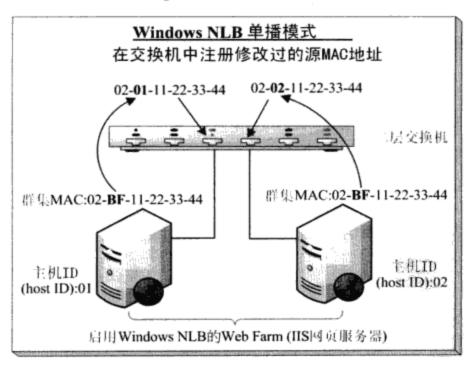


图 7-10

⇒ Switch Flooding的问题

NLB单播模式还有另外一个称为Switch Flooding(交换机泛洪)的问题,以图 7-11为例来 说,虽然交换机每一个port所注册的MAC地址是唯一的,但当路由器接收到要发往群集IP地址

220.10.11.5的数据包时,它会通过ARP协议来查询220.10.11.5的MAC地址,不过它从ARP回复(ARP reply)数据包所获得MAC地址是群集MAC地址02-BF-11-22-33-44,因此它会将此数据包送给MAC地址02-BF-11-22-33-44,然而交换机内并没有任何port注册此MAC地址,因此当交换机收到此数据包时,便会将它发到所有的port,也就出现了Switch Flooding的问题(可先参阅后面附注的说明)。

NLB单播模式的Switch Flooding也可以算是正常现象,因为它让发到此群集的数据包,能够被发到群集中的每一台服务器。不过如果在此交换机上还连接着不隶属于此群集的计算机的话,则Switch Flooding会对这些计算机造成额外的网络负担,甚至会因为其他计算机也收到专属于此群集的机密数据包,而有安全上的顾虑。

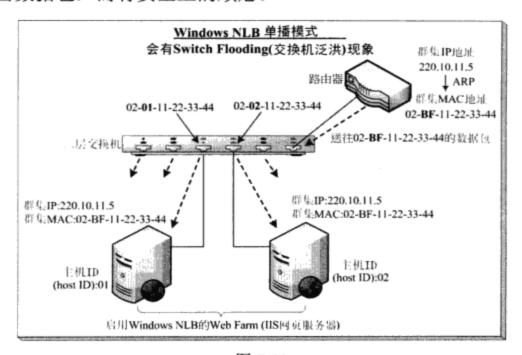


图 7-11

提示

有一种网络攻击行为是将交换机内存储MAC与port对照表的有限内存空间填满,使得交换机无法记录新的对照数据而进入Switch Flooding的状态,造成以后所有收到的数据包都会被广播到所有的port,如此将使得交换机变成与集线器(hub)一样,失去改善网络性能的特点,而且具有机密的数据包被广播到所有port的话,也会让不怀好意者有机会窃取到数据包内的机密文件。

解决Switch Flooding的方法可如图 7-12所示将NLB群集内所有服务器连接到集线器 (hub),然后再将集线器连接到交换机中的一个port,同时禁用前面介绍的MaskSourceMAC功能,这样的话只有这个port会注册群集MAC地址,因此当路由器将目的地为群集MAC地址的数据包发到交换机后,交换机只会通过这个port将它送给集线器,不会干扰到连接在其他port的计算机,而集线器收到此数据包后,就会将它发给群集中的所有服务器(集线器会将所收到的数据包从所有的port发出)。

包 提示

禁用MaskSourceMAC功能的途径为:执行注册表编辑器REGEDIT.EXE,然后将位于以下路径的MaskSourceMAC注册值改为0(数据类型为REG_DWORD):

 $HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \WLBS \Parameters \Interface \Adapter-GUID$

其中的Adapter-GUID为网卡的GUID。

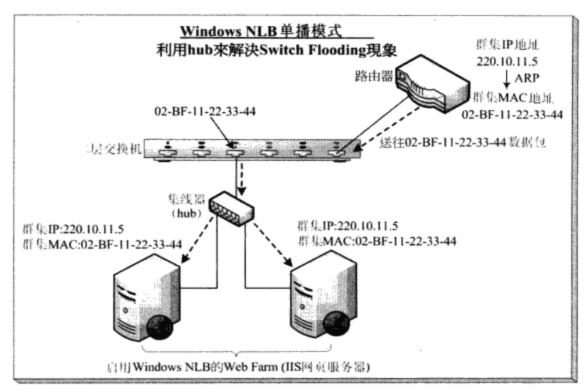


图 7-12

净 提示

您也可以通过交换机的VLAN(虚拟局域网)技术来解决Switch Flooding问题,也就是将NLB群集内所有服务器所连接的port设置为同一个VLAN,以便让NLB群集的流量局限在此VLAN内传送,不会发送到交换机中不属于此VLAN的port。

⇒ 群集服务器之间无法相互通信

如果将网页内容直接放在Web服务器内,并利用**DFS复制**功能来让服务器之间的网页内容一致的话,则采用NLB单播模式还有另外一个的问题:除了与NLB有关的流量之外(例如heartbeat),群集服务器之间无法相互通信。因此群集服务器之间将无法通过**DFS复制**功能来让网页内容一致。

以图 7-13为例来说,当左边服务器要与右边固定IP地址为220.10.11.2的服务器通信时,它会通过ARP请求(ARP Request)数据包来询问其MAC地址,而右边服务器所回复的MAC地址是群集MAC地址02-BF-11-22-33-44,然而这个MAC地址也是左边服务器自己的MAC地址,如此将使得它无法与右边服务器通信。

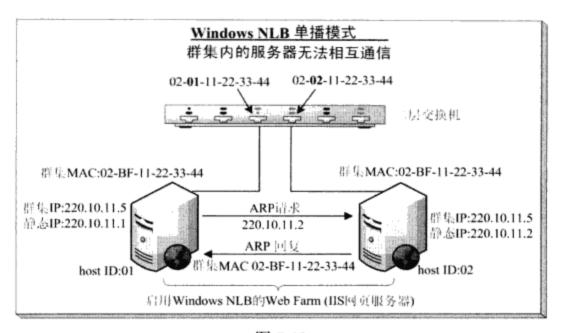


图 7-13

解决群集服务器之间无法相互通信的方法为:如图 7-14所示在每一台服务器各另外安装一块网卡,此网卡不要启用Windows NLB,因此每一台服务器内的这块网卡都会有原来的MAC地址,服务器之间可以通过这些网卡来相互通信。

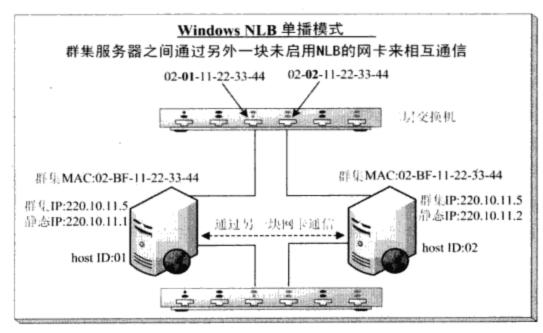


图 7-14

多播模式(multicast mode)

多播的数据包会同时传送给多台计算机,这些计算机都是隶属于同一个**多播组**,它们拥有一个共同的**多播MAC地址**。多播模式具备以下特性:

■ NLB群集内每一台服务器的网卡仍然会保留原来的唯一MAC地址(参见图 7-15),因此群集成员之间可以正常通信,而且在交换机内每一个port所注册的MAC地址就是每台服务器的唯一MAC地址。

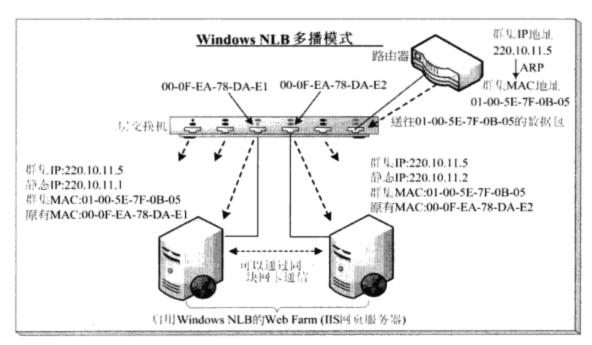


图 7-15

■ NLB群集内每一台服务器还会有一个共享的群集MAC地址,它是一个多播MAC地址,群集内所有服务器都隶属于同一个多播组,并通过这个多播(群集)MAC地址来监听外部的请求。

不过多播模式会有以下的缺点:

■ 路由器可能不支持: 以图 7-15右上角的路由器为例来说,当路由器接收到要发往群集 IP地址220.10.11.5的数据包时,它会通过ARP协议来找询220.10.11.5的MAC地址,而 从ARP回复数据包所获得MAC地址是**多播(群集)MAC地址**01-00-5E-7F-0B-05,路 由器要解析的是"单点"传播地址220.10.11.5,可是所解析到的却是"多点"传送 MAC地址,有的路由器并不接受这样的结果。

解决此问题的方法之一是在路由器内新建静态的ARP映射条目,以便将群集IP地址 220.10.11.5对应到**多播MAC地址**。但若路由器也不支持新建这类型静态数据的话,则 您可能需要更换路由器或改采用单点发送模式。

■ **仍然会有Switch Flooding问题**: 以图 7-15为例来说,虽然交换机每一个port所注册的 MAC地址是唯一的,但当路由器接收到要发往群集IP地址220.10.11.5的数据包时,它 通过ARP协议来查询220.10.11.5的 MAC地址时,所获得的是**多播MAC地址** 01-00-5E-7F-0B-05,因此它会将此数据包发给MAC地址01-00-5E-7F-0B-05,然而交换 机内并没有任何port注册此MAC地址,因此当交换机收到此数据包时便会将它发到所有的port,也因此发生了Switch Flooding现象。

我们在单播模式处,已经介绍过如何解决Switch Flooding的问题,而在多播模式下,还可以通过支持IGMP snooping (Internet Group membership protocol 窥探)的交换机来解决Switch Flooding的问题,因为这类型的交换机会窥探路由器与NLB群集服务器之间的IGMP数据包(加入组、离开组的数据包),如此便可以得知哪一些port所连接的服务器是隶属于此多播组,以后当交换机收到要发到此多播组的数据包时,便只会

将它发往部分port,而这些port所连接的服务器都是隶属于这个多播组。

如果IIS Web服务器只有一块网卡的话,则请选用多播模式。如果Web服务器拥有多块网卡,或网络设备(例如第2层交换机与路由器)不支持多播模式的话,则可以采用单点传播模式。

7-2-4 IIS 7的共享设置

Web Farm内所有Web服务器的设置应该要同步(相同),在旧版IIS中要让服务器之间的设置同步是件麻烦工作,为了解决这个问题,IIS 7提供了**共享设置**功能,它可让您将Web服务器的配置文件存储到远程计算机的共享文件夹内,然后所有Web服务器都可来使用相同的配置文件,这些配置文件包含:

- ApplicationHost.config
 - 这是IIS的主要配置文件,它存储着IIS服务器内所有站点、应用程序、虚拟目录与应用程序集区等设置,同时也存储着服务器的通用默认值。
- Administration.config 存储着委派管理的设置。IIS 7采用模块化设计, Administration.config内也存储着这些 模块的相关数据。
- ConfigEncKey.key

在IIS 7内搭建ASP.NET环境时,有些数据会被ASP.NET加密,例如ViewState、Form Authentication Tickets(窗体验证票)等,此时需要让Web Farm内每一台服务器来使用相同的计算机密钥(machine key),否则当其中一台服务器利用专有密钥将数据加密后,其他使用不同密钥的服务器就无法解密。这些共享密钥是被存储在ConfigEncKey.key文件内。

7-3 实例演练——IIS Web服务器的Web Farm

我们将利用图 7-16来说明如何新建一个由IIS Web服务器所组成的Web Farm,假设其网址为www.sayms.com。我们将直接在图中两台IIS Web服务器上启用Windows NLB,NLB操作模式采用单播模式。

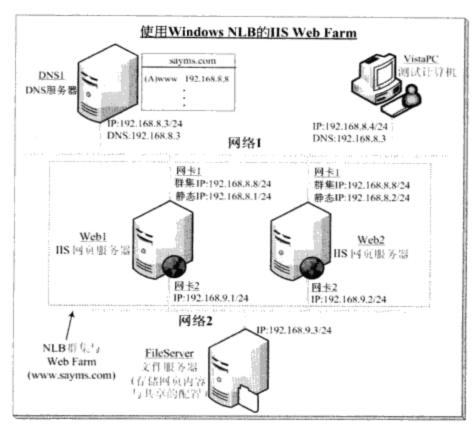


图 7-16

7-3-1 Web Farm的软硬件需求

要新建图 7-16中Web Farm的话,其软硬件配备需符合以下所叙述的要求(建议您利用 Hyper-V所提供的虚拟机来练习,使用Hyper-V的介绍可参考《Windows Server 2008 R2安装与 管理》这本书):

- IIS Web服务器Web1与Web2: 这两台组成Web Farm的服务器都是Windows Server 2008 R2 Enterprise, 且将安装Web服务器(IIS)角色,同时我们要创建一个Windows NLB群集,并将这两台服务器加入到此群集。这两台服务器各有两块网卡,一块连接网络1、一块连接网络2,其中只有网卡1启用Windows NLB,因此网卡1除了原有的固定IP地址(192.168.8.1、192.168.8.2)之外,它们还有一个共同的群集IP地址(192.168.8.8),并通过这个群集IP地址来接收由测试计算机Win7PC发来的上网请求(http://www.sayms.com/)。
- 文件服务器FileServer. 这台Windows Server 2008 R2服务器用来存储Web服务器的网页内容,也就是两台Web服务器的主目录都是在这台文件服务器的相同文件夹。两台Web服务器也应该要使用相同的设置,而这些共享设置也是被存储在这台文件服务器内。

9 提示

由于我们的重点在Web Farm的设置,因此将测试环境简化为仅架设一台文件服务器,故网页内容与共享设置并没有排错功能,您可以自行架设多台文件服务器,然后利用DFS 复制来同步网页内容与共享设置,以便提供排错功能,您也可以利用SAN(FC SAN或 iSCSI SAN)存储设备来存储网页内容与共享设置。关于DFS、iSCSI SAN的介绍与实例演练,请参阅《Windows Server 2008 R2安装与管理》这本书。

- ▶ DNS服务器DNS1: 我们利用这台Windows Server 2008 R2 服务器来解析Web Farm网址www.sayms.com的IP地址。
- ▶ 测试计算机Win7PC: 我们将在这台Windows 7计算机上利用http://www.sayms.com/来测试是否可以正常连接Web Farm网站。若要简化测试环境的话,可以省略此计算机,直接改为通过DNS1来测试也可以。

7-3-2 准备网络环境与计算机

我们将按部就班来说明如何搭建图 7-16中的Web Farm环境,请确实遵照以下步骤来练习,以减少出错的机率。

- ➢ 将DNS1与Win7PC的网卡连接到网络1,Web1与Web2的网卡1连接到网络1、网卡2连接到网络2,FileServer的网卡连接到网络2。若使用Windows Server 2008 R2 Hyper-V虚拟环境的话,请自行新建两个虚拟网络来代表网络1与网络2。
- ▲ 在图中的5台计算机上安装操作系统:除了计算机Win7PC安装Windows 7 (假设是Windows 7 Professional)之外,其他计算机都安装Windows Server 2008 R2 Enterprise,并将它们的计算机名分别改为DNS1、Win7PC、Web1、Web2与FileServer。若是使用Hyper-V虚拟机,而且这5台计算机是从现有虚拟机复制的话,请在这5台计算机上运行Sysprep.exe程序来更改其SID。
- 更改两台Web服务器的两块网卡名称,以便于识别,例如图 7-17表示它们分别是连接到网络1与网络2的网卡:【开始⊃对着网络单击右键⊃属性⊃单击更改适配器设置⊃分别对着两个网络连接单击右键⊃重命名】。

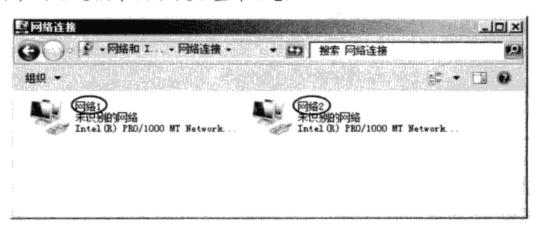


图 7-17

- ▲ 依照实例演练图 (图 7-16) 来设置5台计算机的网卡IP地址、子网掩码、首选DNS服务器(暂时不要设置群集IP地址,等创建NLB群集时再设置,否则IP地址会相冲突):【开始②控制面板②网络和Internet》网络和共享中心②单击本地连接(或网络I、网络2) ②单击属性②Internet协议版本4 (TCP/IPv4)】,本示例采用IPv4。
- 暂时关闭这5台计算机的Windows防火墙(否则下一个测试步骤会被阻止):【开始⊃控制面板⊃系统和安全⊃Windows防火墙⊃查看此计算机已连接的网络位置⊃单击打开或关闭Windows防火墙⊃将计算机所在网络位置的Windows防火墙关闭】。

- → 强烈建议您执行以下步骤来测试同一个子网内的计算机之间是否可以正常通信,以减少后面除错的困难度:
 - 到DNS1上分别用ping 192.168.8.1、ping 192.168.8.2与ping 192.168.8.4来测试是否可以跟Web1、Web2与Win7PC通信。
 - 到Win7PC上分别用ping 192.168.8.1、ping 192.168.8.2与ping 192.168.8.3来测试是否可以跟Web1、Web2与DNS1通信。
 - 到Web1上分别用ping 192.168.8.2 (与ping 192.168.9.2)、ping 192.168.8.3、ping 192.168.8.4与192.168.9.3来测试是否可以跟Web2、DNS1、Win7PC与FileServer通信。
 - 到Web2上分别用ping 192.168.8.1 (与ping 192.168.9.1)、ping 192.168.8.3、ping 192.168.8.4与192.168.9.3来测试是否可以跟Web1、DNS1、Win7PC与FileServer通信。
 - 到FileServer上分别用ping 192.168.9.1与ping 192.168.9.2来测试是否可以跟Web1与Web2通信。

LONG THE RESERVE THE PARTY OF T

≥ 可重新打开这5台计算机的Windows防火墙。

7-3-3 DNS服务器的设置

DNS服务器DNS1是用来解析Web Farm网址www.sayms.com的IP地址。请在其内上安装 DNS服务器角色:【单击左下角服务器管理器图标》 D角色 D添加角色 D单击下一步 D如图 7-18所示选择DNS服务器 D···】。



图 7-18

安装完成后,请通过【开始⊃管理工具⊃DNS⊃对着**正向查找区域**单击右键⊃新建区域】的途径来新建一个名为sayms.com的主要区域,并在这个区域内新建一条Web Farm网址的主机记录,如图 7-19所示,图中假设网址为www.sayms.com,注意其IP地址是群集IP地址192.168.8.8。

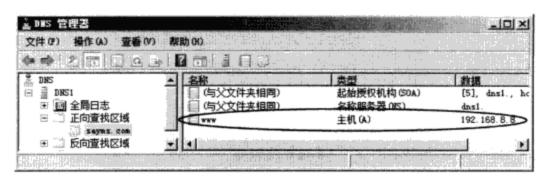


图 7-19

然后到测试计算机Win7PC上来测试是否可以解析到www.sayms.com的IP地址,例如图 7-20为成功解析到群集IP地址192.168.8.8的界面。

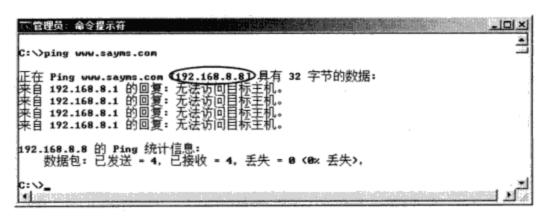


图 7-20

提示

争

虽然成功解析到Web Farm网站的群集IP地址,但是我们还没有新建群集,也还没有设置群集IP地址,故会出现类似无法连接的信息。即使群集与群集IP地址都创建好了,也可能还是会出现类似无法连接的信息,因为Windows Server 2008 R2计算机默认已经启用Windows防火墙,它会阻挡ping命令的数据包。

7-3-4 文件服务器的设置

这台Windows Server 2008 R2文件服务器是用来存储Web服务器的共享设置与共享网页内容。请先在这台服务器的本地安全数据库新建一个用户账户,以便于两台Web服务器可以利用这个账户来连接文件服务器:【开始⊃管理工具⊃计算机管理⊃展开本地用户和组⊃对着用户单击右键⊃新用户⊃如图 7-21所示输入用户名(假设是Webuser)、密码等数据、取消选择用户下次登录时须更改密码、改选择密码永不过期⊃单击创建】。

9 提示

若此台文件服务器有加入Active Directory域的话,则您也可以利用域用户账户。

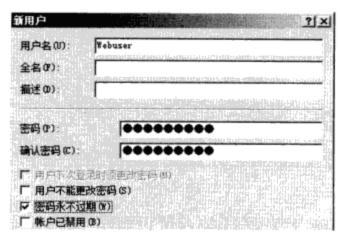


图 7-21

请在此台文件服务器内新建用来存储Web服务器共享设置与网页的文件夹,假设为 C:\Webfiles, 并将其设置为共享文件夹, 假设共享名为Webfiles, 然后开放**读取/写入**(修改) 权限给之前新建的用户Webuser,如图 7-22所示(若出现**网络发现和文件共享窗口**的话,请单 击**是,打开所有公用网络的网络发现和文件共享**)。

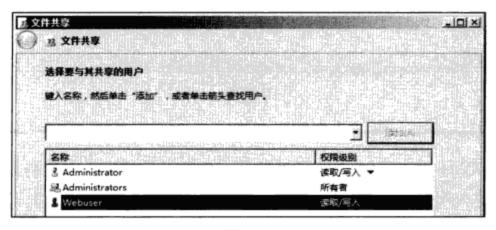


图 7-22

接着在此文件夹内新建两个子文件夹,一个用来存储共享的配置、一个用来存储共享网页 (网站的主目录),假设文件夹名分别是Configurations与Contents,图 7-23为完成后的界面。



图 7-23

7-3-5 Web服务器Web1的设置

我们将在Web1上安装Web服务器(IIS)角色,同时假设网页为使用ASP.NET编写的程序,

因此还需要安装ASP.NET角色服务:【单击左下角服务器管理器图标》 与角色 与添加角色 与单击下一步 与如图 7-24选择Web服务器(IIS) S… O在图 7-25中选择ASP.NET O单击添加必需的角色服务 S… J。完成安装后,我们将使用内置的Default Web Site来作为本演练环境的网站。



图 7-24

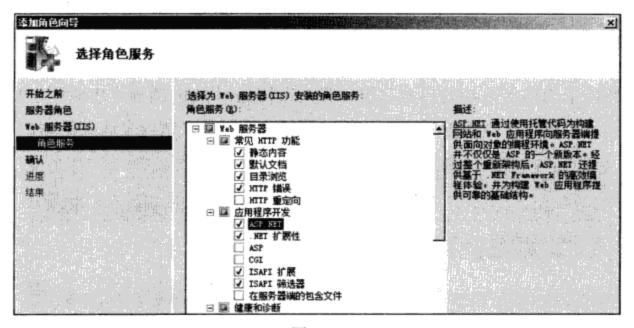


图 7-25

接下来新建一个测试用的首页,假设其文件名为default.aspx,且内容如图 7-26所示,将此文件放到网站默认的主目录%*SystemDrive*%\inetpub\wwwroot之下,其中的%*SystemDrive*%一般是C:。

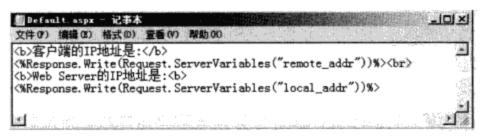


图 7-26

建议更改网站读取默认文件的优先级,以便让网站优先读取default.aspx,其设置途径为: 【如图 7-27所示单击Default Web Site ⊃单击中间的默认文档 ⊃选择default.aspx ⊃通过单击右边 操作窗格的上移,来将default.aspx调整到列表的最上方】,它可以提高首页访问效率,避免网 站浪费时间去尝试读取其他文件。



图 7-27

接着请到测试计算机Win7PC上利用浏览器来测试是否可以正常连接网站与看到默认的网 页,如图 7-28所示为连接成功的界面,图中我们直接利用Web1的固定IP地址192.168.8.1来连 接Web1, 因为我们还没有启用Windows NLB, 无法使用群集IP地址来连接网站。

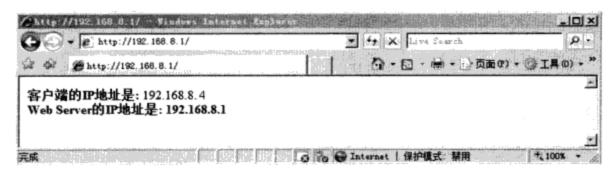


图 7-28

7-3-6 Web服务器Web2的设置

Web2的设置步骤大致上与Web1的设置相同,以下仅列出摘要:

- ▲ 在Web2上安装Web服务器(IIS)角色与ASP.NET角色服务。
- "不需要"新建default.aspx、也"不需要"将default.aspx复制到Web2的主目录
- ☑ 直接到测试计算机Win7PC上利用http://192.168.8.2/来测试Web2网站是否正常运行,由 于Web2并没有另外新建default.aspx首页,故在Win7PC上测试时,所看到的界面是默 认的首页,如图 7-29所示。



图 7-29

注意

如果您所架设的Web Farm是SSL网站的话,则请在Web1完成SSL证书申请与安装步骤、将SSL证书导出存档、到Web2上通过Internet Information Services (IIS)管理器来将此证书导出到Web2的网站。

7-3-7 共享网页与共享的配置

接下来我们要让两个网站使用存储在文件服务器FileServer内的共享网页与共享的配置。

Web1共享网页的配置

我们将以Web1的网页来当作两个网站的共享网页,因此请先将Web1主目录C:\inetpub\wwroot内的测试首页default.aspx。通过网络复制到文件服务器FileServer的共享文件夹\\FileServer\Webfiles\Contents内:[开始与运行争输入\\FileServer\Webfiles\Contents 后单击确定与如图 7-30所示将Default.aspx复制到此共享文件夹内】。

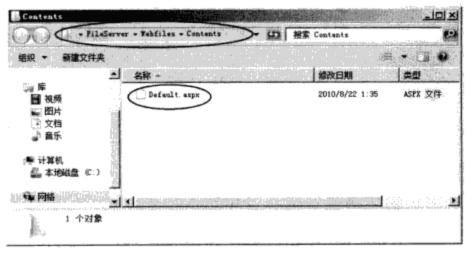


图 7-30

注意

在Windows Server 2008 R2内启用了网络发现功能后,可能也会像图 7-30一样在网络上看 不到FileServer这台计算机,其可能原因是**网络发现**功能又被自动关闭了(可通过【开始 ⊃对着网络单击右键⊃属性⊃单击更改高级共享配置】来查看),而其可能原因是以下四 个服务没有启动: DNS Client、Function Discovery Resource Publication、SSDP Discovery、 UPnP Device Host。若要在Web1上可以通过网络看到服务器FileServer的话,请将Web1 与FileServer这两台计算机的以上四个服务都启动。

接下来要将Web1的主目录指定到\\FileServer\Webfiles\Contents共享文件夹,并且利用新建 在文件服务器FileServer内的本地用户账户Webuser来连接此共享文件夹,不过在Web1上也必须 新建一个相同名与密码的用户账户(请取消选择用户下次登录时须更改密码、改选择密码永 **不过期**),且必须将其加入到**IIS IUSRS**组内,如图 7-31所示。

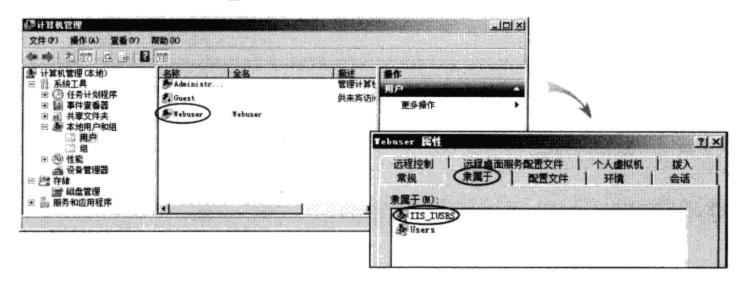


图 7-31

将Web1主目录指定到\\FileServer\Webfiles\Contents共享文件夹的步骤为:

STEP 1 如图 7-32所示单击Default Web Site右边的基本设置。

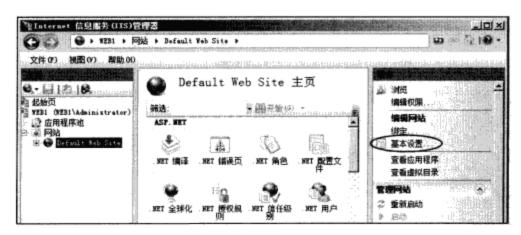


图 7-32

STEP 2 如图 7-33所示在**物理路径**处输入\\FileServer\Webfiles\ Contents、单击连接为。

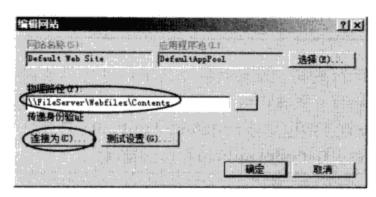


图 7-33

STEP 3 在图 7-34中【选择**特定用户⊃**单击设置⊃输入用来连接共享文件夹的用户名 Webuser与密码⊃依次单击确定】。

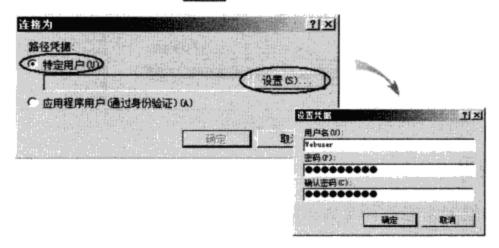


图 7-34

STEP 4 单击图 7-35中的测试设置,测试是否可以正常连接上述共享文件夹,前图所示为正常连接的界面。单击确定。

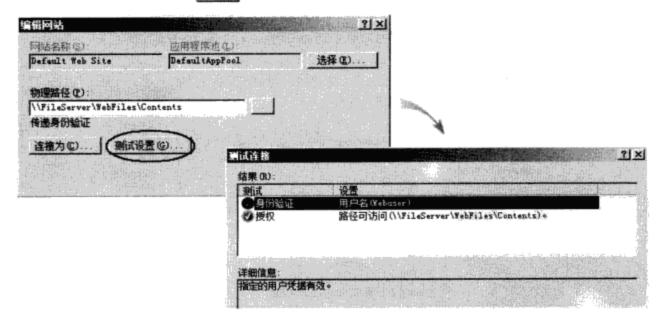


图 7-35

完成后,请到测试计算机Win7PC上利用http://192.168.8.1/来测试(建议先将浏览器的缓存清除),此时应该可以正常看到default.aspx的网页。

包 提示

如果网站因故不正常运行或安全设置有异动的话,则您可能需要针对网站所在的应用程序池来执行回收(recycle)操作,以便让网站恢复正常或取得最新的安全设置值。举例来说,Default Web Site的应用程序池为DefaultAppPool,若要针对此池来执行回收操作的话,请如图 7-36所示单击DefaultAppPool右边的回收...。

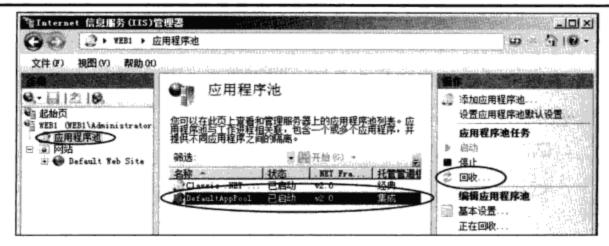


图 7-36

Web1的共享的配置

我们将以Web1的设置来当作两个Web服务器的共享设置,因此请先将Web1的设置与密钥导出到 \\FileServer\Webfiles\Configurations, 然后再指定Web1来使用这份位于\\FileServer\Webfiles\Configurations的设置。

STEP 1 将 Webl 的设置导出、存储到\\FileServer\Webfiles\Configurations 内。请双击 图 7-37 服务器 WEBl 界面中的**共享的配置**。



图 7-37

STEP 2 单击图 7-38中右边的**导出配置...**。

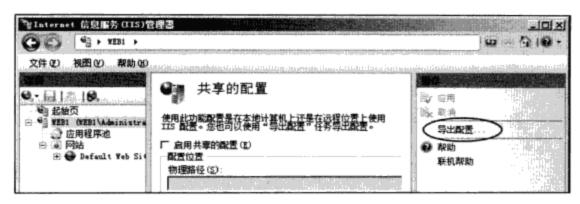


图 7-38

STEP 3 请【在图 7-39后图的**物理路径**中输入用来存储共享的配置的共享文件夹 \\FileServer\WebFiles\Configurations ⊃单击**连接为** ⊃输入有权限连接此共享文件 夹的用户名(Webuser)与密码 ⊃单击确定】。

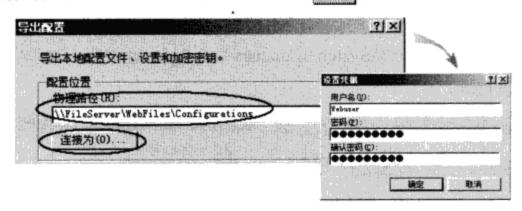


图 7-39

STEP 4 在图 7-40中【设置用来保护加密密钥的密码⊃单击确定⊃在前图中单击确定】,密码必须至少8个字符,且需包含数字、特殊符号、英文大小写字母。

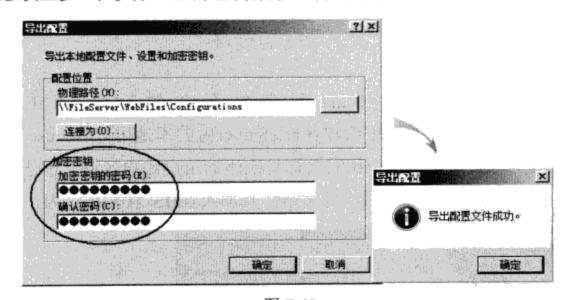


图 7-40

STEP 5 接着启用Web1的共享的配置功能:【在图 7-41中选择启用共享的配置⊃在物理路径中输入存储共享的配置的路径\\FileServer\WebFiles\Configurations⊃输入有权限连接此共享文件夹的用户名(Webuser)与密码⊃单击应用⊃在前图中输入保护加密密钥的密码⊃单击确定】。



图 7-41

STEP 6 由图 7-42后图可知, Web1的现有加密密钥会被备份到本地计算机内用来存储设置的目录中(%Systemroot%\System32\inetsrv\config)、由前图可知需要关闭,然后重新启动IIS管理器。

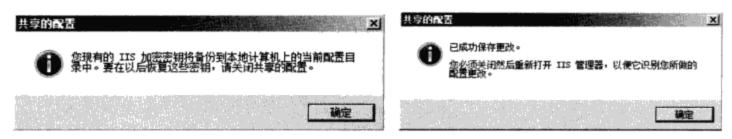


图 7-42

完成后,请到测试计算机Win7PC上利用http://192.168.8.1/来测试(建议先将浏览器的缓存清除),此时应该还是可以正常看到default.aspx的网页。

Web2共享网页的设置

我们要将Web2的主目录指定到文件服务器FileServer的共享文件夹 \\FileServer\Webfiles\Contents,并利用新建在FileServer内的本地用户Webuser来连接此共享文件夹,不过在Web2上也必须新建一个相同名称与密码的用户账户(请取消选择用户下次登录时须更改密码、改选择密码永不过期),且必须将其加入到IIS_IUSRS组内,如图7-43所示。

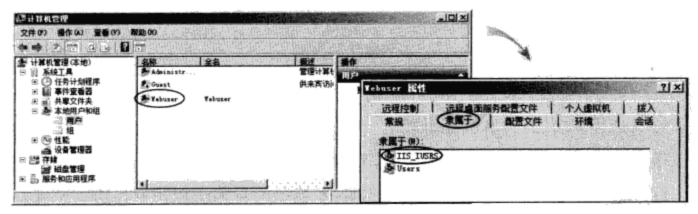


图 7-43

将Web2的主目录指定到\\FileServer\Webfiles\Contents共享文件夹的步骤与Web1完全相



同,此处不再重复,查看图 7-44与图 7-45。

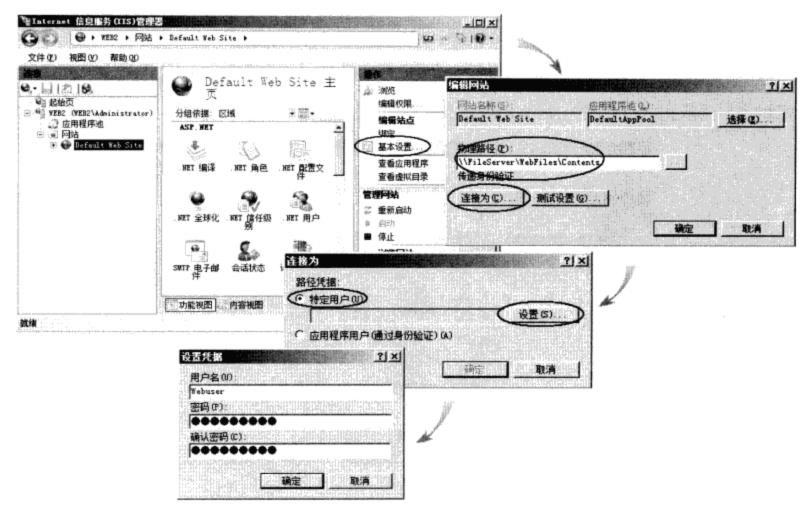


图 7-44



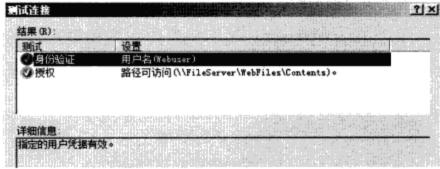


图 7-45

完成后,请到测试计算机Win7PC上利用http://192.168.8.2/来测试(建议先将浏览器的缓存清除),此时应该还是可以正常看到default.aspx的网页,如图 7-46所示。建议更改Web2默认文件的优先级(将default.aspx移动到最上面),以便提高首页访问效率。

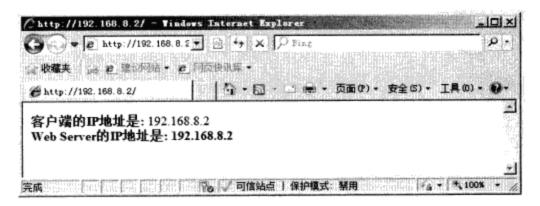


图 7-46

Web2的共享的配置

现在我们要让Web2来使用位于\\FileServer\Webfiles\Configurations内的共享的配置(这些设置是之前从Web1导出到此处的),其步骤如下所示。

STEP 1 请双击图 7-47服务器WEB2界面中的共享的配置。



图 7-47

STEP 2 在图 7-48中【选择启用共享的配置⊃在物理路径中输入存储共享的配置的路径\\FileServer\WebFiles\Configurations⊃输入有权限连接此共享文件夹的用户名(Webuser)与密码⊃单击应用⊃在前图中输入保护加密密钥的密码⊃单击确定]。

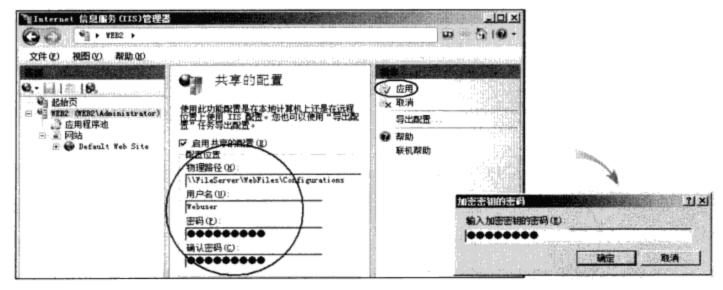


图 7-48

STEP 3 由图 7-49可知, Web2的现有加密密钥会被备份到本地计算机内用来存储设置的目录中(%Systemroot%\System32\inetsrv\config),需要关闭然后重新启动IIS管理器。

图 7-49

完成后,请到测试计算机Win7PC上利用http://192.168.8.2/来测试(建议先将浏览器的缓存清除),此时应该还是可以正常看到default.aspx的网页。

7-3-8 创建Windows NLB群集

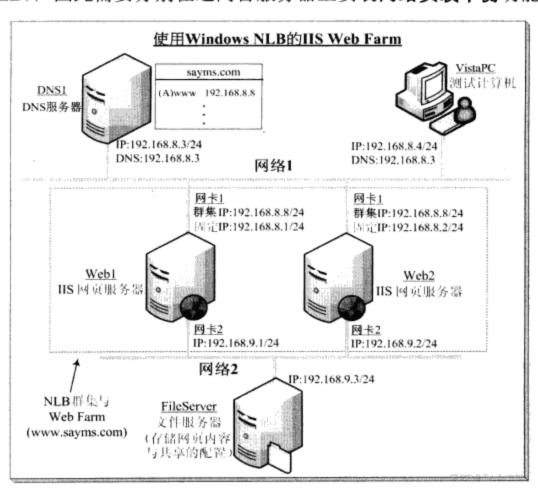


图 7-50

创建Windows NLB群集的步骤如下所示:

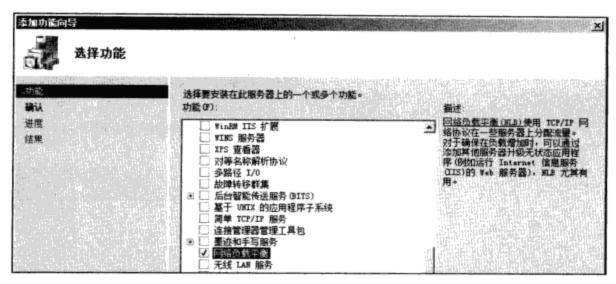


图 7-51

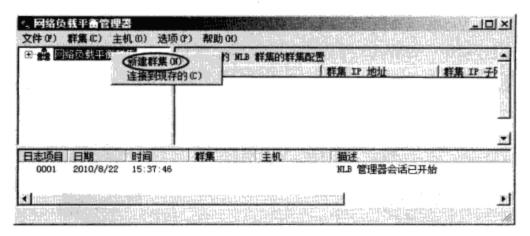


图 7-52

STEP 3 在图 7-53的**主机**处输入要加入群集的第1台服务器的计算机名Web1后单击连接,然后从界面下方选择Web1内欲启用NLB的网卡后单击下一步。图中我们选择连接在网络1的网卡。

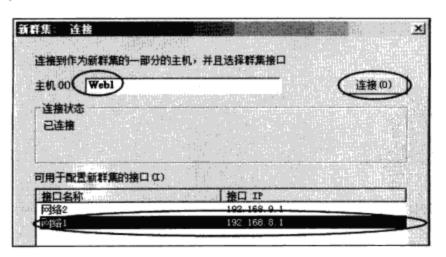


图 7-53

STEP 4 在图 7-54中直接单击 下一步即可。图中的**优先级(单一主机标识符)**就是web1的 host ID(每一台服务器的host ID必须是唯一的),若群集接收到的数据包是未定义 在**端口规则**内的话,它会将此数据包交给优先级较高(host ID数字较小)的服务器

来处理。您也可以在此界面为此网卡添加多个IP地址。

IP 地址		子网攬码	
192. 168. 8. 1	Willian de lieuring	255. 255. 255.	9
hiddens IC Jaan II Indich (15 15 15 15 16 16	Stelan owall constrain	er en	OMESIA O DESIGNATO SE

图 7-54

STEP 5 在图 7-55单击添加、设置群集IP地址(例如192.168.8.8)与子网掩码(255.255.255.0) 后单击确定。

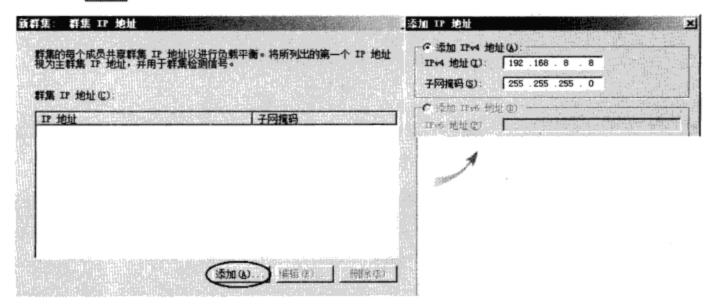


图 7-55

STEP 6 回到新群集: 群集IP地址界面时单击下一步(您也可以在此处添加多个群集IP地址)。 STEP 7 在图 7-56中直接单击下一步。图中群集操作模式我们选择单播模式。

群集 IP 配置 IP 地址(A):	192 168 8 8
子网攬码(S):	255 255 255 0
完整 Internet 名称(F):	A DESCRIPTION OF THE PROPERTY
网络地址 (2):	02+hf-c0+s8-08-08
群集操作模式(0)	
(C 单播(U)	

图 7-56

② 提示

您也可以选择**多播**或**IGMP多播**,若选择**IGMP多播**的话,群集中的每台服务器会定期送出**IGMP加入组**的信息,支持**IGMP Snooping**的交换机收到此信息后,就可得知这些隶属于相同多播组的群集服务器是连接在哪一些port上,如此便可以将Switch Flooding限制在这些port上。

STEP 8 在图 7-57中直接单击完成来采用默认的端口规则。

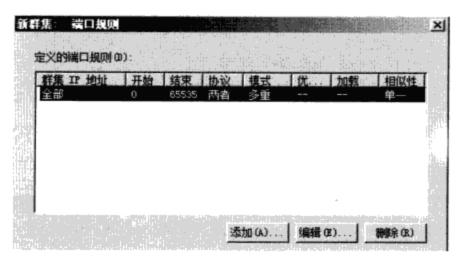


图 7-57

STEP 9 设置完成后会进入**聚合**(convergence)程序,稍待一段时间后便会完成此程序,而图 7-58中**状态**列也会改为图中的**已聚合**。

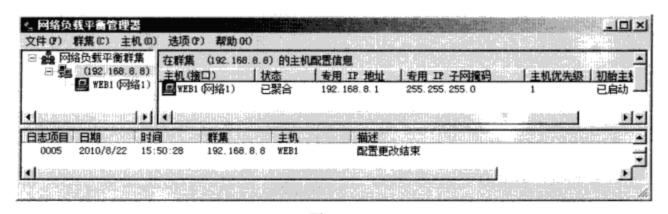


图 7-58

STEP 10 接下来将Web2加入到NLB群集:如图 7-59所示【对着群集IP地址192.168.8.8单击右键 □添加主机到群集 □在主机处输入Web2后单击连接 □从界面下方选择Web2内要启用NLB的网卡后单击下一步(图中我们选择连接在网络1的网卡)】。

学 注意

请先将Web2的Windows防火墙关闭或例外开放文件和打印机共享,否则会因Windows防火墙的阻止而无法解析到Web2的IP地址。若不想变动Windows防火墙设置的话,请直接输入Web2的IP地址。

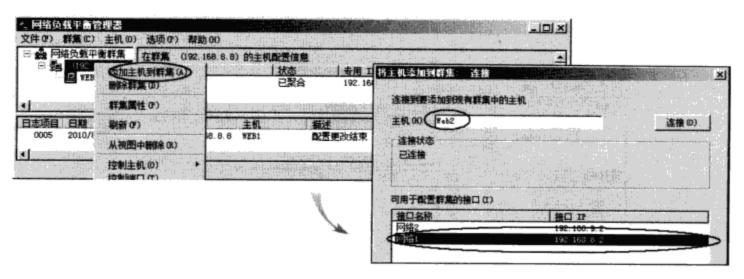


图 7-59

STEP 11 在图 7-60中直接单击下一步即可,其优先级(单一主机标识符)为2,也就是host ID 为2。

用 IP 地址 (1)	子网攬码		
192.168.8.2		255, 255, 255, 0	
V			
	添加 (A)	编辑 (2)	勝線 (R)

图 7-60

STEP 12 在图 7-61中直接单击完成。

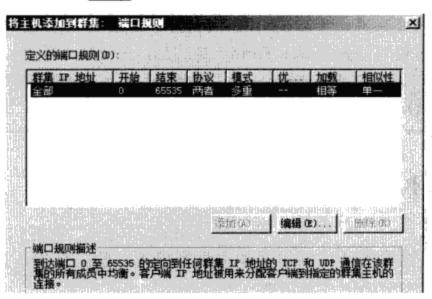


图 7-61

STEP 13) 设置完成后便进入聚合(convergence)程序,WEB2中的状态列也会改为已聚合,

如图7-62所示。

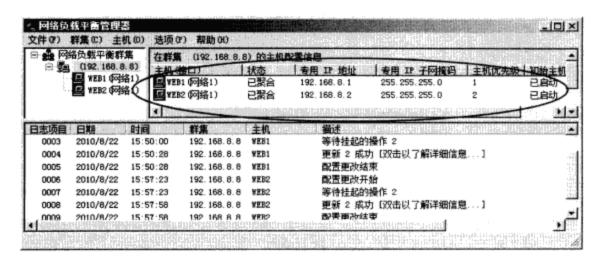


图 7-62

完成以上设置后,接下来请到测试计算机Win7PC上利用浏览器测试是否可以连接到Web Farm网站,这一次我们将如图 7-63通过网址www.sayms.com来连接,此网址在DNS服务器内所记录的IP地址为群集的IP地址192.168.8.8,故此次是通过NLB群集来连接Web Farm,图 7-63 为成功连接后的界面。

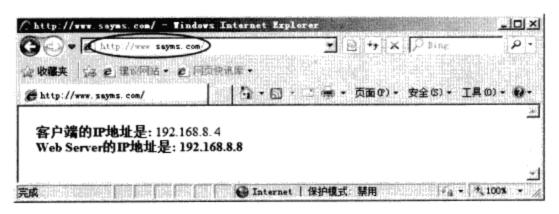


图 7-63

9 提示

您可以利用以下方式来进一步测试NLB与Web Farm功能。将Web1关机,但保持Web2开机,然后再测试是否可以连接Web Farm。完成后,改为Web2关机,但保持Web1开机,然后再测试是否可以连接Web Farm。为了避免Internet Explorer缓存干扰您验证实验结果,因此每次测试前,请先删除缓存文件。

7-4 Windows NLB群集的高级管理

如果您要更改群集设置的话,例如添加主机到群集、删除群集,请如图 7-64所示对着群集单击右键,然后通过图中的选项来设置。



图 7-64

您也可以针对单一服务器来更改其设置,其设置途径为如图 7-65所示对着服务器单击右键,然后通过图中的选项来设置。图中的**删除主机**会将该服务器从群集中删除,并禁用其**网络负载平衡**功能。

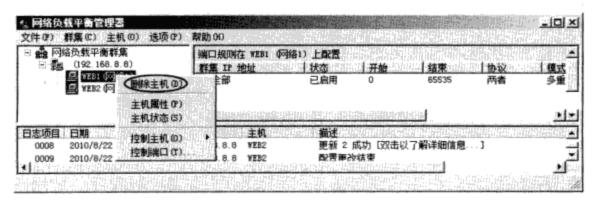


图 7-65

图 7-64中选择**群集属性**,就可以通过图 7-66来更改群集IP地址、群集参数与端口规则。

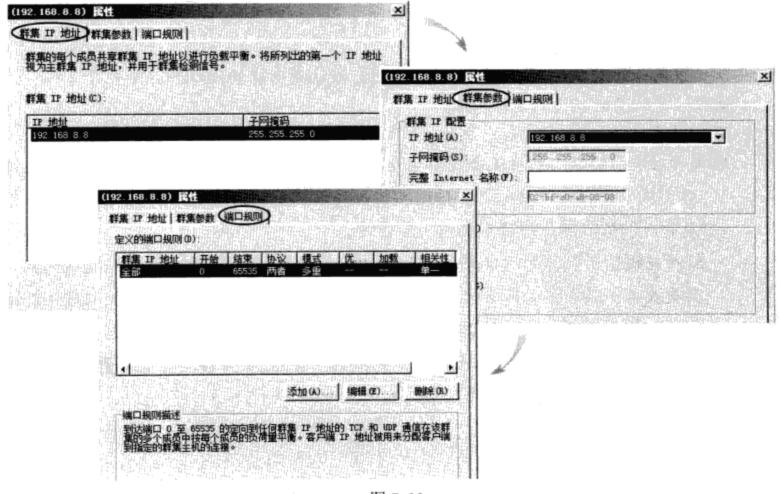


图 7-66

此处我们针对端口规则来做进一步的说明。请选择图中唯一的端口规则后按**编辑**,此时会出现如图 7-67所示的界面。



图 7-67

- 群集IP地址:通过此处来选择适用此端口规则的群集IP地址,也就是只有通过此IP地址来连接NLB群集时,才会应用此规则。
 - 如果此处是选择**全部**的话,则所有群集IP地址都适用于此规则,此时这个规则被称为 **通用端口规则**。如果您自行添加了其他端口规则,而其设置与**通用端口规则**相冲突的 话,则您添加的规则优先。
- ≥ 端口范围: 此端口规则所涵盖的端口范围, 默认是所有的端口。
- 协议: 默认同时包含TCP与UDP。
- 🍱 筛选模式
 - **多个主机**: 群集内所有服务器都会处理进入群集的网络流量,也就是共同来提供网络负载平衡与排错功能,并依照相似性的设置来将请求交给群集内的某台服务器负责。相似性的原理请参阅前面所介绍。

针对此规则所涵盖的端口来说,群集中每一台服务器的负担比率默认是相同的,若要更改单一服务器的负担比率的话,请【对着该服务器单击右键D主机属性D端口规则标签D选择端口规则D单击编辑 D在图 7-68中先取消选择相等后、再通过负荷量来调整相对比率】。举例来说,如果群集中有3台服务器,其负荷量值分别是50、100、150,则其负担比率为1: 2: 3。

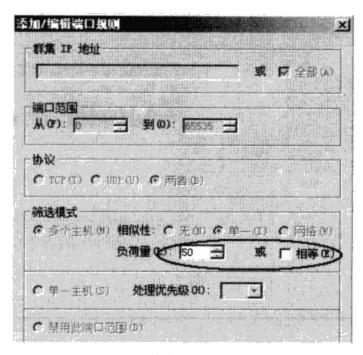


图 7-68

- 单一主机:表示与此规则有关的流量都将交给单一服务器来负责处理,这台服务器是处理优先级(handling priority)较高的服务器,处理优先级默认是根据host ID来设置(数字较小优先级越高)。您可以更改服务器的处理优先级值(参考图 7-69中的处理优先级)。
- 禁用此端口范围:则所有与此端口规则有关的流量都将被NLB群集阻挡。

您可以通过【如图 7-69所示对着服务器单击右键⊃控制主机】的途径来启动(开始)、停止、排出停止、挂起与继续该台服务器的服务。其中的**停止**会让此服务器停止处理所有的网络流量请求,包含正在处理中的请求;而**排出停止**(drainstop)仅会停止处理新的网络流量请求,但是目前正在处理中的请求并不会被停止。

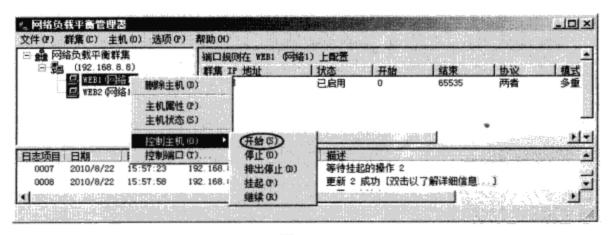


图 7-69

您可以通过【如图 7-70对着服务器单击右键②控制端口②选择端口规则】的途径来启用、禁用或排出该端口规则。其中的**禁用**表示此服务器不再处理与此规则有关的网络流量,包含正在处理中的请求;而**排出**(drain)仅会停止处理新的网络流量请求,但是目前正在处理中的请求并不会被停止。

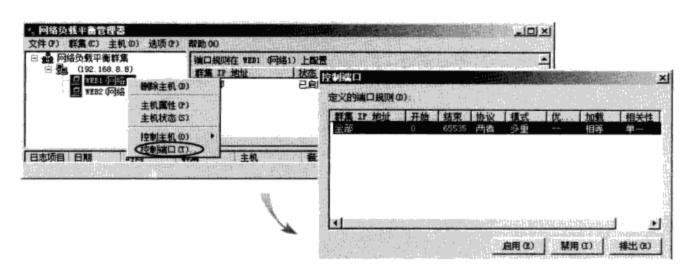


图 7-70



您也可以利用NLB.EXE程序来执行上述的管理工作。