### Creating and Configuring Web Sites in Windows Server 2003





**Recommended Sites** 



Internet Information Services 6 (IIS 6) is a powerful platform for hosting web sites on both the public Internet and on private intranets. Creating and configuring web sites and virtual directories are bread-and-butter tasks for IIS Administrators, and in this article we'll walk through the process of doing this using both the GUI (IIS Manager) and using various scripts included with Windows Server 2003. The seven specific tasks we'll walk through will include:

5/11/2005



- Creating a Web Site
- Creating a Local Virtual Directory
- Creating a Remote Virtual Directory
- Controlling Access to a Web Site
- Configuring Web Site Logging
- Configuring Web Site Redirection
- Stopping and Starting Web Sites

For sake of interest, we'll explain these tasks in the context of a fictitious company called TestCorp as it deploys IIS for its corporate intranet.

### **Preliminary Steps**

Unlike earlier versions of Microsoft Windows, IIS is not installed by default on Windows Server 2003. To install IIS, open Manage Your Server from the Start menu and add the Application Server role:



Note that for simple security reasons IIS should only be installed on member servers, not domain controllers. The reason is that if you install IIS on a domain controller and your web server becomes compromised, the attacker could gain access to your accounts database and wreak havoc with your network.

# **Creating a Web Site**

The simplest approach is to use a separate IP address to identify each web site on your machine. Let's say our server has five IP addresses assigned to it from the range 172.16.11.220 through 172.16.11.224. Before we create a new Human Resources web site, let's first examine the identify of the Default Web Site. Open IIS Manager in Administrative Tools, select Web Sites in the console tree, and right-click on Default Web Site and open it's properties:

Documence 1	Directory Security HTTP Headers Custom Error
Web Site	Performance ISAPI Filters Home Directory
Web site identifi	cation
Description:	Default Web Site
IP address:	(All Unassigned)
ICP port:	80 SSL port:
Enable HTTP	Y Keep-Alives
Enable loggi	ng mat:
✓ Enable loggi Active log for W3C Extend	ng mat: ed Log File Format <u>P</u> roperties
✓ Enable loggi Active log for W3C Extend	ng mat: ed Log File Format <u>P</u> roperties

The IP address for the Default Web Site is All Unassigned. This means any IP address not specifically assigned to another web site on the machine opens the Default Web Site instead. A typical use for the Default Web Site is to edit it's default document to display general information like a company logo and how to contact the Support Desk.

Let's use IP address 172.16.11.221 for the Human Resources site and make D:\HR the folder where the home page for this site is stored. To create the HR site, right-click on the Web Sites node and select New --> Web Site. This starts the Web Site Creation Wizard. Click Next and type a description for the site:

eb Site Creation Wizard			
Web Site Desciption Describe the Web site to help adminis	trators identify it.		(Ind)
Type a description of the Web site.			
<u>D</u> escription:			
Human Resources			
	< <u>B</u> ack	<u>N</u> ext >	Cancel
	-		61

Click Next again and specify 172.16.11.221 as the IP address for the site:

Enter the IP address to use for	this Web site:	
172.16.11.221	¥	
(All Unassigned) 172.16.11.220 172.16.11.223		
172.16.11.222 172.16.11.221 172.16.11.224		

Click Next and specify D:\HR as the home folder for the site. We've cleared the checkbox to deny anonymous access to the site because this is an internal intranet so only authenticated users should be able to access it (public web sites generally allow anonymous access):

Web Site Creation Wizard		×
Web Site Home Directory The home directory is the root of your V	Web content subdirectories.	E Star
Enter the path to your home directory.		
<u>P</u> ath:	<u>ب</u>	
D:\HR		B <u>r</u> owse
Allow anonymous access to this W	eb site	
	< <u>B</u> ack <u>N</u> ext>	Cancel

Click Next and leave only Read access enabled since the Human Resources site will initially only be used to inform employees of company policies:

Web Site Creation Wizard			×
Web Site Access Permissions Set the access permissions for this Web	site.		
Allow the following permissions:			
<b>☞</b> <u>Read</u>			
Run scripts (such as ASP)			
Execute (such as ISAPI applications	or CGI)		
□ <u>W</u> rite			
E Browse			
To complete the wizard, click Nex	ıt.		
	< <u>B</u> ack	<u>N</u> ext >	Cancel
	101		101 107

Click Next and then Finish to create the new web site:

Internet Information Services (I	IS) Manager			
🕤 Eile Action View Window H	elp			_ <b>B</b> ×
← → 🗈 🖬 🗙 🗗 🔂	1 😰 💂 🕨 🔳	Ш		
M Internet Information Services	Name	Path	Status	
Application Pools     Web Sites     Default Web Site     Human Resources     Web Service Extensions				
		1	J	

Now let's create another intranet site, this time for Help Desk, which will use IP address 172.16.11.222 and home folder D:\Help. We'll create this one using a script instead of the GUI:

Command Pro	mpt	_O×
C:\>iisweb / Connecting t Server Site Name Metabase Pat IP Host Port Root Status	Create D:\Help "Help Desk" /i 172.16.11.222 o serverDone. = TEST220 = Help Desk h = W3SUC/1181955842 = 172.16.11.222 = NOT SPECIFIED = 80 = D:\Help = STARTED	
C:\>		<b>•</b>

And here's the result:

Internet Information Services	(IIS) Manager			
S Elle Action View Window	Help			_ <b>8</b> ×
	) <mark>않</mark> 및 ▶ I	. 11		
M Internet Information Services	Name	Path	Status	
Application Pools     Application Pools	erauk.ntm			
		J	1	

The script we used here is Iisweb.vbs, one of several IIS administration scripts available when you install IIS on Windows Server 2003. The basic syntax of this script is easy to figure out from the previous screenshot, and a full syntax can be found here. Note that unlike the Web Site Creation Wizard used previously. you can't use this script create a web site with anonymous access disabled. So if you want to disable anonymous access you should do it by opening the properties sheet for the Help Desk site, selecting the Directory Security tab, and clicking the Edit button under Authentication and Access Control. This opens the Authentication Methods box where you can clear the checkbox to disable Anonymous Access and leave Windows Integrated Authentication as the only authentication

method available for clients on your network:

lser name:	TUSB TEST220	Browse
eassword:		
Authenticated For the followi	access ng authentication methods, us	er name and passw
are required w - anor - acce Integrated	vhen: hymous access is disabled, or iss is restricted using NTFS acc I Wi <u>n</u> dows authentication	ess control lists
are required w - anor - acce ✓ Integrated Digest aut	vhen: hymous access is disabled, or iss is restricted using NTFS acc I Wi <u>n</u> dows authentication hentication for Windows doma	ess control lists in servers
are required w - anor - acce Integrated Digest auth Basic auth	when: hymous access is disabled, or iss is restricted using NTFS acc I Windows authentication hentication for Windows doma entication (password is sent in	ess control lists in servers clear text)
are required w - anor - acce Integrated Digest auth Basic auth .NET Pass	when: hymous access is disabled, or iss is restricted using NTFS acc I Windows authentication hentication for Windows doma entication (password is sent in port authentication	ess control lists in servers clear text)
are required w - anor - acce ✓ Integrated ✓ Digest auth ─ Basic auth	vhen: hymous access is disabled, or iss is restricted using NTFS acc I Windows authentication hentication for Windows doma entication (password is sent in	ess control lists in servers clear text)

# **Creating a Local Virtual Directory**

Let's say Human Resources keeps their policies in a folder called D:\HR Policies on your web server and you would like users to be able to use the URL http://172.16.11.221/policies when they need to access these policies. To do this we need to create a virtual directory that associates the /policies portion of the URL, called the alias for the virtual directory, with the physical directory D:\HR Policies where these documents are actually located.

Let's do this now. Right-click on the Human Resources site and select New --> Virtual Directory to start the Virtual Directory Creation Wizard. Click Next and type the alias for the virtual directory:

Virtual Directory Creation Wizard		×
Virtual Directory Alias Specify a short name, or alias, for th	is virtual directory.	
Type the alias you want to use to ga same naming conventions that you Alias:	ain access to this Web virtual directo would for naming a directory.	ry. Use the
1 million and a second		
	< <u>B</u> ack <u>N</u> ext>	Cancel

Click Next and specify the physical folder on the local server to map to this alias:

ual Directory Creation Wizard			
eb Site Content Directory Where is the content you want to put	blish on the Web sil	e?	BILL
Enter the path to the directory that co	intains the content	for this Web site.	
<u>P</u> ath:			
D:\HR Policies			Browse
	< Back	Next>	Cancel

Click Next and specify permissions (again we'll just leave Read enabled) and finish the wizard. Here's the result:

Internet Information Services	(IIS) Manager			
Sile Action View Window	Help			_ <b>8</b> ×
	) 🕜 🔍 🕨 🗉	I II		
Internet Information Services	Name	Path	Status	
Application Pools  Application Pools  Web Sites  Human Resources  Policies  Help Desk Web Service Extensions	default.htm policy1.htm policy2.htm policy3.htm			
			<u></u>	[

Let's do something similar using another IIS script named Iisvdir.vbs, only we'll create a /procedures virtual directory instead:



Open IIS Manager to display the new virtual directory:

Internet Information Services		_O×		
Elle Action View Window	Help			_ <b>5</b> ×
		• •	Tari	
Internet Information Services     Application Pools     Application Pools     Web Sites     Default Web Site     Default Web Site	Policies	D:\HR Policies D:\HR Procedures	Status	

Note the difference in the icons for the two virtual directories. That's because when the script creates a virtual directory it also creates an application starting point for that directory, while the wizard does not. This doesn't matter though, since for now we're only hosting static content in these directories. For the full syntax of Iisvdir.vbs see here.

### **Creating a Remote Virtual Directory**

Help Desk likes to do things differently than Human Resources does, and their user manual is stored in HTML form in the share \\srv230\helpdesk on a network file server. Let's create a remote virtual directory within the Help Desk site that associates the alias /usermanual with this share. Right-click on the Help Desk site and select New --> Virtual Directory to start the Virtual Directory Creation Wizard again, specify usermanual as the alias for the directory, and type \\srv230\helpdesk as the UNC path to the share:

Virtual Directory Creation Wizard	×
Web Site Content Directory Where is the content you want to publish on the Web site?	
Enter the path to the directory that contains the content for this Web s Path:	ite.
\\172.16.11.230\helpdesk	B <u>r</u> owse
< <u>B</u> ack <u>N</u> ext >	Cancel

Click Next and a new screen appears prompting you to either specify credentials for accessing the share or use the authenticated user's credentials for this purpose (we'll use the latter):

ecurity Credentials Specify a user name ar network resource.	nd password to prevent unauthorized access (	to the
Enter the user name ar directory.	nd password that should be used to gain acce	ss to the network
	Browse	
Password:		
Always use the aut access to the netw	henticated user's credentials when validating ork directory.	
		-

Click Next and finish the wizard. Let's look at the result:

• → 🖻 🖬 🗙 🛱 🖸 🖡	3 2 2 1	■ II		
Internet Information Services	Name	Path	Status	
Application Pools     Sites     Default Web Site     Muman Resources	efault.htm		R fa	

The Iisvdir.vbs script can similarly be used for creating remote virtual directories.

### **Controlling Access to a Web Site**

Now that we have a couple of web sites and virtual directories created, let's look at a few administration tasks. This will be only a brief overview--you can find a much more detailed treatment of the subject in my book IIS 6 Administration (Osborne/McGraw-Hill).

First let's look at how we can control access to our web sites. There are basically four ways you can do this: NTFS Permissions, web permissions, IP address restrictions, and authentication method. NTFS permissions is your front line of defense but it's a general subject that we can't cover in detail here. Web permissions are specified on the Home Directory tab of your web site's properties:

http://www.windowsnetworking.com/articles\_tutorials/Web-Sites-Windows-2003.html 5/11/2005

Documents	Directory Security	HTTP Headers	Custom Error
Web Site	Performance I	SAPI Filters	Home Directory
The content for thi	s resource should come fr	om:	
	A directory located or	this computer	
	• A share located on an	other computer	
	A redirection to a <u>URL</u>		
Lo <u>c</u> al path:	D:\HR		Browse
The second s		. <del></del>	
Write     Directory brows     Application settings	ing		1
Write Directory brows Application settings Application name:	Ing		Remove
<u>Write</u> Directory <u>b</u> rows     Application settings     Application name:     Starting point:	ing Default Application	>	Remove
<u>Write</u> Directory <u>b</u> rows     Application settings     Application name:     Starting point:     Execute <u>permission</u> :	ing Default Application <human resources<br="">:: None</human>	>	R <u>e</u> move Configuration
<u>Write</u> Directory <u>b</u> rows     Application settings     Application name:     Starting point:     Execute <u>permission</u> :     Application pool:	ing Default Application <human resources<br="">None DefaultAppPool</human>	>	R <u>e</u> move Configuration
<u>Write</u> Directory <u>b</u> rows     Application settings     Application na <u>m</u> e:     Starting point:     Execute <u>p</u> ermission:     Application pool:	ing Default Application <human resources<br="">:: None DefaultAppPool</human>	>	Remove Configuration Unload

By default only Read permission is enabled, but you can also allow Write access so users can upload or modify files on your site.

Script source access so users can view the code in your scripts (generally not a good idea), or Directory browsing so users can view a list of files in your site (also not a good idea). Web permissions apply equally to all users trying to access your site, and they are applied before NTFS permissions are applied. So if Read web permission is denied but NTFS Read permission is allowed, users are denied access to the site.

IP address restrictions can be used to allow or deny access to your site by clients that have a specific IP address, have an IP address within a range of addresses, or have a specific DNS domain name. To configure this, select the Directory Security tab and click the Edit button under IP Address and Domain Name Restrictions. This opens the following dialog, which by default does not restrict access to your site:

y default,	all computers will be:	Granted access	
xcept the f	ollowing:	🔒 🔿 Denied access	
Access	IP address (Subnet	mask)	
			Add
			Remove
			Edi <u>t</u>

The main thing to watch for here is that denying access based on domain name involves reverse DNS lookups each time clients try to connect to your web site, and this can significantly impact the performance of your site.

The final way of controlling access to your sites is to use the Authentication Methods dialog box we looked at previously:

Jse the followi	ng Windows user account for	anonymous access:
Jser name:	IUSR_TEST220	Browse,
eassword:	*******	
where	arress	
For the following required with a required with a required with a required with a recent of the following required with a required to the requ	ng authentication methods, us hen: ymous access is disabled, or ss is restricted using NTFS acc Windows authentication pentication for Windows doma entication (password is sent in port authentication	er name and passwor ess control lists in servers clear text)
For the following are required w - anon - acce ✓ Integrated Digest auth Basic authe .NET Passp	actors ong authentication methods, us hen: ymous access is disabled, or ss is restricted using NTFS acc Windows authentication entication for Windows doma entication (password is sent in ort authentication	er name and passwor ess control lists in servers clear text) Select

In summary, the five authentication options displayed here are:

- Anonymous access. Used mainly for web sites on public (Internet) web servers.
- Integrated Windows authentication. Used mainly for web sites on a private intranet.
- Digest authentication. Challenge/response authentication scheme that only works with clients running

Internet Explorer 5.0 or later.

- **Basic authentication**. Older authentication scheme that transmits passwords over the network in clear text, so use this only in conjunction with SSL.
- .NET Passport authentication. Allows users to use their .NET Passport for authentication.

## **Configuring Web Site Logging**

Since web sites are prime targets for attackers, you probably want to log hits to your site to see who's visiting it. By default IIS 6 logs traffic to all content as can be seen on the bottom of the General tab of the properties for a web site or virtual directory:

Documents	Directory Security HTTP Headers Custom Errors
Web Site	Performance ISAPI Filters Home Directory
Web site identif	ication
Description:	Human Resources
IP address:	172.16.11.221 💌 Advanced
ICP port:	80 SSL port:
Enable logo	ping
Enable logo Acti <u>v</u> e log fo W3C Exten	ging ormat: ded Log File Format
- I Enable logg Acti <u>v</u> e log fo W3C Exten	ging ormat: ded Log File Format
✓ Enable log( Acti <u>v</u> e log fo W3C Exten	ging ormat: ded Log File Format
✓ Enable logg Acti <u>v</u> e log fo W3C Exten	ging ormat: ded Log File Format

The default logging format is the W3C Extended Log File Format, and clicking Properties indicates new log files are created daily in the indicated directory. It's a good idea to specify that local time be used for logging traffic as this makes it easier to interpret the logs:

New log schedule <ul> <li>Hourly</li> <li>Daily</li> <li>Weekly</li> <li>Monthly</li> <li>Unlimited file size</li> <li>When file size reaches:</li> <li>20</li> <li>MB</li> </ul> <li>Isse local time for file naming and rollover</li> <li>Log file directory:</li> <li>C:\WINDOWS\system32\LogFiles</li> <li>Browse</li>	operal	1			
New log schedule         C Hourly         Daily         Weekly         Monthly         Unlimited file size         When file gize reaches:         20         MB             Use local time for file naming and rollover         Log file directory:         C:\WINDOWS\system32\LogFiles         Browse         Log file name:         W35VC1525757177\exyymmdd.log	enerai	Advanced			
<ul> <li>C Hourly</li> <li>Daily</li> <li>Quekly</li> <li>Monthly</li> <li>Unlimited file size</li> <li>When file size reaches:</li> <li>20</li> <li>MB</li> </ul> ✓ Use local time for file naming and rollover Log file directory: C:\WINDOWS\system32\LogFiles Browse Log file name: W3SVC1525757177\exyymmdd.log	-New I	og schedule			
O Daily     O Weekly     Monthly     O Unlimited file size     When file size     When file size reaches:     20     P MB     Use local time for file naming and rollover     Log file directory:     C:\WINDOWS\system32\LogFiles     Browse Log file name:     W35VC1525757177\exyymmdd.log	C	Hourly			
○ Weekly         ○ Monthly         ○ Unlimited file size         ○ When file size reaches:         20       →         20       →         Ø       Use local time for file naming and rollover         Log file directory:       Erowse         C:\WINDOWS\system32\LogFiles       Erowse         Log file name:       W3SVC1525757177\exyymmdd.log	•	Daily			
<ul> <li>C Monthly</li> <li>C Unlimited file size</li> <li>C When file size reaches:</li> <li>20 → MB</li> <li>✓ Use local time for file naming and rollover</li> <li>Log file directory:</li> <li>C:\WINDOWS\system32\LogFiles Browse</li> <li>Log file name: W35VC1525757177\exyymmdd.log</li> </ul>	C	<u>W</u> eekly			
♥ Unlimited file size         ♥ When file size reaches:         20       #         Ø       Use local time for file naming and rollover         Log file directory:	C	Monthly			
♥ When file size reaches:         20       →         Ø       Use local time for file naming and rollover         Log file directory:	C	Unlimited file size			
20       MB         Image: Second system       MB         Image: Main Second system       MB         Image: Second system       MB	C	When file size read	hes:		
✓       Use local time for file naming and rollover         Log file directory:		20 -	MB		
✓ Use local time for file naming and rollover         Log file directory:         C:\WINDOWS\system32\LogFiles         Browse         Log file name:       W3SVC1525757177\exyymmdd.log		,	Concerning of the second se		
Log file directory:          C:\WINDOWS\system32\LogFiles       Browse         Log file name:       W3SVC1525757177\exyymmdd.log	🔽 Use	local time for file na	ming and rollove	r	
C:\WINDOWS\system32\LogFiles <u>B</u> rowse Log file name: W35VC1525757177\exyymmdd.log	Log file	directory:			
Log file name: W35VC1525757177\exyymmdd.log	C:\WI	NDOW5\system32\L	.ogFiles		Browse
Log file name: W3SVC1525757177\exyymmdd.log	1				-
	Log file	name: W3SVC	I1525757177\ex	yymmdd.log	
		1.16	L ancel L	LIDDIV .	Hein

The key of course is to review log files regularly to look for suspicious activity. IIS doesn't include anything for this purpose, but the IIS 6.0 Resource Kit Tools does include version 2.1 of Microsoft Log Parser, which can be used for analyzing IIS logs. You can download these tools here.

## **Configuring Web Site Redirection**

Sometimes you need to take your web site down for maintenance, and in such cases it's a good idea to redirect all client traffic directed to your site to an alternate site or page informing users what's going on. IIS lets you redirect a web site to a different file or folder on the same or another web site or even to an URL on the Internet. To configure redirection you use the Home Directory tab and choose the redirection option you want to use:

	Directory Security HTTP Heade	rs Custom Errors
Web Site	Performance ISAPI Filters	Home Directory
The content for this	s resource should come from:	
	C A directory located on this compute	r
	A share located on another comput	er
	A redirection to a <u>U</u> RL	
Redire <u>c</u> t to:	http://srv240/sitedown.htm	_
The client will be ser	nt to:	
The exact URL e	entered above	
- · · · · · ·		
A directory belo	w URL entered	
A directory belo	w URL entered direction for t <u>h</u> is resource	
A directory belo	w URL entered direction for t <u>h</u> is resource	
A directory belo	w URL entered direction for t <u>h</u> is resource Default Application	Remove
A directory belo Application settings Application name: Starting point:	w URL entered direction for t <u>h</u> is resource Default Application <human resources=""></human>	R <u>e</u> move
A directory belo Application settings Application name: Starting point: Execute permission:	w URL entered direction for this resource Default Application <human resources=""></human>	Remove Configuration
A directory belo Application settings Application name: Starting point: Execute permission:	w URL entered direction for t <u>h</u> is resource Default Application <human resources=""> s: None</human>	Configuration
A directory belo Application settings Application name: Starting point: Execute permission: Application pool:	w URL entered direction for this resource Default Application <human resources=""> s: None DefaultAppPool</human>	Configuration Configuration
A directory belo A permanent re Application settings Application name: Starting point: Execute germission: Application pool:	w URL entered direction for t <u>h</u> is resource Default Application <human resources=""> s: None DefaultAppPool</human>	Configuration

## **Stopping and Starting Web Sites**

Finally, if sites become available you may need to restart IIS to get them working again. Restarting IIS is a last resort as any users currently connected will be disconnected and any data stored in memory by IIS applications will be lost. You can restart IIS using IIS Manager by right-clicking on the server node:

Internet Information Se	rvices (IIS) Manager			
G Elle Action View Wir	ndow Help			_ <b>5</b> ×
	₿ 8 \$ •	11		
Internet Information Service	Name		Status	
IEST220 (local comput     Application Pools     Web Sites     Default Web S     Human Resour	Connect Disconnect Browse	nsions	Service is running	
	New	6		
🖃 🔛 Help Desk	All Tasks 🔹 🕨	Backup/Resto	ore Configuration	
Web Service Exter	View	Restart IIS Save Configu	raSion to Disk	
Shutdown, and/or restart Inte	Refresh Export List			
producting and/or resource into	Properties		1	1
	Help			

You can also do the same from the command-line using the Iisreset command:



Type **iisreset /?** for the full syntax of this command. You can also start and stop individual web sites using IIS Manager or the Iisweb.vbs script. And you can stop or start individual IIS services using the net commands, for example **net stop w3svc** will stop the WWW services only.

### Summary

In this article I've explained how to create and configure web sites and virtual directories on IIS 6. Most of what we've covered also applies to IIS 5 on Windows 2000 as well. In the next article I'll delve into creating and configuring FTP sites and implementing FTP User Isolation, a new feature of Windows Server 2003. For a deeper look at IIS 6 see my book IIS 6 Administration (Osborne/McGraw-Hill).

### **About Mitch Tulloch**



Mitch Tulloch is a writer, trainer and consultant specializing in Windows server operating systems, IIS administration, network troubleshooting, and security. He is the author of 15 books including the <u>Microsoft Encyclopedia of Networking</u> (Microsoft Press), the <u>Microsoft Encyclopedia of Security</u> (Microsoft Press), <u>Windows Server Hacks</u> (O'Reilly), <u>Windows Server 2003 in a Nutshell</u> (O'Reilly), <u>Windows 2000 Administration in a Nutshell</u> (O'Reilly), and <u>IIS 6 Administration</u> (Osborne/McGraw-Hill). Mitch is based in Winnipeg, Canada, and you can find more information about his books at his website <u>www.mtit.com</u>

**Click here** for Mitch Tulloch's section.

### Check out these recent articles by Mitch Tulloch

- May 10, 2005, Key Performance Monitor Counters
- Apr 21, 2005, Troubleshooting Startup Problems
- Apr 12, 2005, Book Reviews: Security Books
- Apr 05, 2005, Implementing Fault Tolerance on Windows Networks
- Mar 22, 2005, Terminal Services Group Policy

Click here for more articles by Mitch Tulloch.

### Get new article updates in your Inbox

Get all the various Windows networking related articles about setting up Windows NT/XP/2000/2003 networks, troubleshooting, connectivity and more delivered directly to your mailbox as and when they are released on WindowsNetworking.com by signing up to our Real-Time Article Update below.

Email a	ddress:*
---------	----------

Subscribe

\* Please note that we do NOT sell or rent the email addresses belonging to our subscribers; we respect your privacy!

http://www.windowsnetworking.com/articles\_tutorials/Web-Sites-Windows-2003.html 5/11/2005

#### Featured Links\*

- 75% of attacks are on web applications. Secure your apps with **Acunetix Web Vulnerability Scanner.** 

- Control Portable Storage Devices - Network-wide control with LANguard PSC. - Dld Today

**- Free Download** - Detect & Correct network & server issues automatically with GFI Network Server Monitor

- Find thousands of essential tips in our WindowsNetworking.com Windows NT/2000/2003/XP Admin Knowledge Base!

Join our mailing list! Enter your email below, then click the "join list" button

Admin KnowledgeBase | Articles & Tutorials | Authors | Hardware | Links | Message Boards | Newsletters | 📧 | Software

About Us : Contact Us : Product Submission Form : Advertising Information WindowsNetworking.com is in no way affiliated with Microsoft Corp. \*Links are sponsored by advertisers. Copyright © 2005 TechGenix Ltd. All rights reserved. Please read our online privacy statement.