NetWare* Web Server* Contents


Overview


How Do I . . .


Windows

Trademarks

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Overview

A Web server is a program running on one computer that fulfills requests for documents from other computers running Web client programs (also called browsers). The World Wide Web (WWW) is a global network of computers running Web servers.

A Web client requests a document from a Web server by sending a HyperText Transfer Protocol (HTTP) request that identifies the document by Uniform Resource Locator (URL). Although the document can consist of any type of information, including text, graphics, sound files, or other multimedia elements, documents created specifically for the WWW are usually formatted using the HyperText Markup Language (HTML).

The NetWare* Web Server* is a NetWare Loadable Module* (NLM*) that integrates a NetWare server into the existing WWW environment as a Web server. From the NetWare Web Server, you can publish documents to the NetWare and Internet user communities over a TCP/IP network.

The NetWare Web Server enables you to

- Customize the Web server configuration to your specific environment
- Publish documents
- Control who accesses the documents on your server
- Track activity on your server
- Create dynamic Web pages

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

NetWare* Web Server* Configuration

After you install the NetWare Web Server software, there are no required configuration tasks. The Web server is functional as soon as the NLM* programs are loaded.

If you wish, you can customize Web server performance by modifying the server parameters.

- You can modify the basic server configuration parameters using the NetWare Web Server Windows** administration utility.
- You can modify the advanced server configuration parameters by editing the NetWare Web Server configuration files manually.

You can also modify the NetWare server configuration to

- Tune system performance when multiple application NLMs are run on the server.
- Set up long file name support for Java** applets.

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Document Publishing

To make the Web pages (documents) you create available everywhere on the WWW, you must publish them.

To publish documents on the NetWare* Web Server*, store the documents on the server's file system in the location set aside for Web documents. The part of the server's file system that is set aside for Web documents is called the document tree. The top of the document tree is called the document root.

To publish documents on the NetWare Web Server, you can

- Store your Web pages in existing directories in the default document tree
- Set up a home page for your Web server
- Create new directories in the document tree in which to store Web documents

In addition to simply storing documents in the document tree, you can set up additional features to customize your tree.

- You can set up basic document tree features using the NetWare Web Server Windows** administration utility.
- You can set up more advanced document tree features by editing the NetWare Web Server configuration files yourself.

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Transaction Logging

The NetWare* Web Server* monitors all HTTP requests and responses and generates log files detailing these transactions. These log files are valuable for monitoring how often users access the Web server and which files are most commonly retrieved. The files can also help you identify server errors and locate the source of possible attacks on your server.

Although the Web server automatically generates log files whenever the server is running, you can change the level of logging and the number and size of the log files. Perform all log file management tasks, including setting logging options and viewing, saving, and printing the log files, using the NetWare Web Server administration utility.

Access Control

If your Web server is connected to the Internet, any Web client anywhere in the world can retrieve the documents stored in the document tree. If there is information in your document tree that you do not want to be readily available to the rest of the world, you must restrict access to your server.

Access control determines who can access the information on your server. You can restrict access to all of the information or restrict it directory by directory. An access control entry can control access for user groups, usernames, IP networks, IP addresses, domain names, or hostnames.

When the Web server receives an HTTP request, it locates the requested file to obtain its pathname. It then checks to see if access control has been set up for any of the directories in the path. If access control has been set up for any one of the directories, the server identifies the source of the request. It then determines whether the source is allowed access according to the controls set for the directory.

You can set up access control for any of the directories in the document tree using the NetWare* Web Server* administration utility.

Dynamic Web Pages

A Web client can directly access any of the documents stored as files in your document tree. Such documents are referred to as static Web pages because the contents of the document change only if authors manually modify the files. Static Web pages usually contain the same information every time a client requests them. Static Web pages are useful as home pages and for publishing corporate literature, marketing materials, or other information that changes infrequently.

The Web server can also respond with dynamic Web pages, pages that are created on the fly in response to a specific client request. If you want your Web server to serve dynamic Web pages, you must create custom extensions. You can create extensions by writing BASIC or Perl scripts or by writing your own NLM* programs.

The NetWare* Web Server* uses the Remote Common Gateway Interface (RCGI) to communicate between the Web server and BASIC or Perl extensions. It uses the Local Common Gateway Interface (LCGI) to communicate with NLM extensions. RCGI and LCGI are based on the Common Gateway Interface (CGI), the standard in UNIX** Web server implementations. You can learn how to write your own RCGI extensions by reading the Dynamic Web Page Programmer's Guide.

HyperText Transfer Protocol (HTTP)

The protocol that defines how the Web server and the Web client communicate. To provide for the fastest possible response times, HTTP calls for a simple client-server transaction as follows:

1. A Web client opens a connection with a Web server.
2. The Web client sends a request to the Web server. The client request includes header information that may identify the type of browser initiating the transaction and the types of documents the client understands.
3. The Web server sends a response that includes a status code indicating whether the request was successful and the actual data (document) requested, if available. The Web server returns a header that provides information such as the number of bytes transferred and the type of document returned.
4. The Web server or the Web client closes the connection. HTTP only allows for one request per connection.

HyperText Markup Language (HTML)

A document formatting language that is used to create Web pages. Unlike files created in word processing or desktop publishing applications that require a specific application and platform to be recognizable, HTML documents are suitable for viewing on any platform. This is because an HTML document is simply a text file with special tags embedded in the text that describe what a block of text is, not what it should look like. The task of formatting a specific block of text is left up to each Web browser that retrieves the HTML document.

HTML is also provides a way of linking to other documents from within a document. This linking of documents is what enables people to "surf" the Web.

Uniform Resource Locator (URL)

An address that identifies a single Web document. Every Web document has its own URL, which identifies the protocol, address, port number, and location of the file. If no port number is specified, port 80 (the default HTTP port) is assumed.

For example, the URL

http://www.novell.com/whatnew/whatnew.htm

identifies a document that can be accessed by sending an HTTP request to port 80 on host www.novell.com. The document, whatnew.htm, resides in the /whatnew directory in the document tree that has been set up for the Web server.

IP Address

A unique address that identifies a system on a TCP/IP network. The IP address is represented as a 4-byte address in standard dotted decimal notation. The bytes are decimal, hexadecimal, or octal values separated by periods (for example, 123.45.6.7). A partial IP address might include the first one, two, or three bytes of the address (for example, 123, 123.45, or 123.45.6).

Hostname

A unique name associated with an IP address. A hostname cannot contain a space, tab, number sign (#), or end-of-line character.

Alias

An alternative name for a system. Typically, an alias is shorter than the formal hostname. For example, host john.galaxy.com might also be known simply as john. In this case, john is an alias. A single host can have from one to ten aliases.

Domain Name System

A standardized naming service that provides information about hostname and IP address mapping throughout an internetwork. DNS maintains this information in a decentralized distributed database.

DNS Domain

A group of networked computers under common DNS management. Domains can be determined by logical grouping instead of physical location. The domain naming scheme reflects the structure of the DNS hierarchy. A domain name is simply a list of all domains in the path from the local domain to the root. Each label in the domain name is delimited by a period, or dot (.). For example, marketing.company1.com is a fully qualified domain name; host1.marketing.company1.com is a fully qualified DNS hostname.

DNS Name Server

A server that contains a database of information about hosts in one or more DNS domains and makes this information available to DNS clients, or resolvers, throughout the network.

Port

In TCP/IP, a well-known point of access to a service on a host computer. Certain ranges of port numbers are usually assigned to the same services by convention. Other ranges are available for use as needed by applications.

Name Resolution

The process by which an IP address is translated into a hostname. The NetWare* Web Server* can perform resolution either by looking for an IP address-to-hostname mapping in its SYS:ETC\HOSTS file or by sending a request to a DNS name server.

*Novell trademark. ** Third-party trademark. Use Index for trademark information.

Document Root

The directory at the top level of the directory structure that is the document tree. All documents published on the NetWare* Web Server* must be stored in the document root directory or one of its subdirectories. WWW clients cannot access documents that are located in a directory above the document root directory.

Server Root

The top of the directory structure containing Web server files. By default, the server root directory is SYS:WEB. The Web server looks for its document root (DOCS), log file (LOGS), and configuration file (CONFIG) directories relative to the server root. The server root is defined by the ServerRoot directive in the HTTPD.CFG file.

Image Map Configuration File

An image map configuration file correlates a shape and its coordinates on a graphics file with a particular URL. When a user clicks an active area, or hotspot, on an image map, the Web server compares the coordinates of the spot to the coordinates in the image map configuration file and redirects the client to the corresponding URL.

Format

The NetWare* Web Server* supports the standard NCSA image map configuration file format. Each line in the map file looks like this:

shape /URL a,b x,y

- *shape* is the shape of the hotspot.

  The shape can be rect (rectangle), circle, poly (polygon), or point (which instructs the server to redirect the client to the URL that corresponds to the nearest hotspot when the user clicks outside the bounds of a defined hotspot).

- *URL* is the URL to which the client is directed when the user clicks on the defined hotspot.
- *a*,*b x*,*y* are the coordinates of the shape that represents the hotspot.

  The coordinates are measured from the upper left corner of the image and are represented in pixels. Rectangles have two pairs of coordinates (for the upper left and lower right corners of the rectangle). Circles have two pairs of coordinates (one for the center point of the circle and one for any point along the circle's circumference). Polygons have as many pairs of coordinates as needed.

An Example

The following line in an image map configuration file instructs the server to direct the client to the /IMAGES/GIF4.HTM file whenever a user clicks on the area of the image map defined by a rectangle with coordinates 150,2 318,82:

rect /images/gif4.htm 150,2 318,82

Multimedia Internet Mail Extensions (MIME) Type

A convention used to map a data type to a particular filename extension. A MIME-type header is sent with every Web document to describe the content of the document. Web browsers use the MIME type to determine what to do with the document.

Automatic Directory Indexing

A feature that enables the Web server to generate an index automatically whenever a client sends a URL that identifies a directory instead of a specific file. Automatic directory indexing must be enabled for a directory before the Web server can generate an index. Automatic directory indexing is useful when the contents of a directory change often or when a directory contains many files.

Fancy Indexing

An automatic directory indexing feature that enables the Web server to generate index entries that show icons, file size information, and file descriptions in addition to filenames.

Icons are links

An automatic directory indexing feature that enables the Web server to create index entries in which icons displayed with a given filename are active links to the associated document. When the user clicks on an icon, the browser is automatically redirected to the URL for the associated filename.

Scannable Titles

An automatic directory indexing feature that enables the Web server to generate a description for each file in the directory by scanning the HTML documents for titles. While this is a useful feature, it should be used sparingly because it requires significant server processing resources that can affect performance.

Server-Side Include (SSI)

A mechanism that enables the Web server to modify HTML documents slightly before sending them to a requesting client. The changes the Web server makes are controlled by SSI commands embedded in the HTML document. For example, there are SSI commands that instruct the Web server to include another file in the HTML file or print information about the file. HTML documents that contain SSI commands must use the .SSI filename extension and must be stored in a directory that has the server-side include feature enabled.

include Command

Use the include command to insert an HTML or text document into the current document at the include command. You can only insert documents that are stored on the local server.

The include command supports two tags:

- file, which allows you to identify the file to include using a path and filename that are relative to the current directory (the directory containing the SSI document)
- virtual, which allows you to identify the file to include using a path and filename that are relative to the document root (SYS:WEB/DOCS by default)

The include command uses the following syntax:

<!--#include file|virtual="*filename*"-->

For example, to include the file /WEB/DOCS/SSI/NEWDOC.HTM in the file /WEB/DOCS/SSI/SSIDOC.SSI, type either of the following commands into the SSIDOC.SSI file:

<!--#include file="newdoc.htm"-->

or

<!--#include virtual="/ssi/newdoc.htm"-->

echo Command

Use the echo command to print information about the current document. For example, you can use the echo command to instruct the Web server to include the document name or last modification date in the document.

The echo command uses the following syntax:

<!--#echo var="*environment_variable*"-->

The *environment variable* can be any of the following:

- DOCUMENT_NAME, which is the document filename.
- DOCUMENT_URI, which is the document's Universal Resource Identifier (URI). This is equivalent to the pathname of the document.
- DATE_LOCAL, which is the current date and time.
- DATE_GMT, which is the current Greenwich Mean date and time.
- LAST_MODIFIED, which is the date and time the document was last modified.
- REMOTE_ADDR, which is the IP address of the client requesting the document.
- SERVER_SOFTWARE, which is the name and version of the Web server software.
- SERVER_NAME, which is the local hostname of the Web server.
- SERVER_PORT, which is the TCP port on which the Web server is listening for HTTP requests.
- REMOTE_HOST, which is the hostname of the requesting client.
- AUTH_TYPE, which is the method used to authenticate user requests.
- REMOTE_USER, which is the username of the client who sent the request.

For example, to include the current date and time in an HTML document, type the following in the HTML document:

The current date and time is <!--#echo var="DATE_LOCAL"-->

flastmod Command

Use the flastmod command to include the date on which either the current file or another file was last modified in the current document.

The flastmod command supports two tags.

- file, which allows you to identify the file using a path relative to the current directory (the directory containing the SSI document)
- virtual, which allows you to identify the file using a path relative to the document root (/WEB/DOCS by default)

The flastmod command uses the following syntax:

<!--#flastmod file|virtual="*filename*"-->

For example, to include the last modification date of the file /WEB/DOCS/SSI/STOCKQT.HTM in the /WEB/DOCS/SSI/SSIDOC.SSI, you can type either of the following commands into the SSIDOC.SSI file:

<!--#flastmod file="stockqt.htm"-->

or

<!--#flastmod virtual="/ssi/stockqt.htm"-->

By default, the last modification date is displayed in the standard date and time format (for example, Tuesday, 09-Jan-96 09:00:00 PDT). If you want to customize the date and time format, use the flastmod command with the config command.

fsize Command

Use the fsize command to include the size of the current file or another file in the current document.

The fsize command supports two tags.

- file, which allows you to identify the file using a path relative to the current directory (the directory containing the SSI document)
- virtual, which allows you to identify the file using a path relative to the document root (/WEB/DOCS by default)

The fsize command uses the following syntax:

<!--#fsize file|virtual="*filename*"-->

For example, to include the size of the file /WEB/DOCS/SSI/BIGFILE.GIF in the /WEB/DOCS/SSI/SSIDOC.SSI, type either of the following commands into the SSIDOC.SSI file:

<!--#fsize file="bigfile.gif"-->

or

<!--#fsize virtual="/ssi/bigfile.gif"-->

By default, the file size is displayed in kilobytes. To display the file size in bytes, use the fsize command in conjunction with the config command.

config Command

Use the config command to change the format of the file size returned by the fsize command or the date and time returned by the flastmod command. You can also use the config command to customize the action the server takes when it encounters an SSI error.

The config command supports four tags.

- sizefmt, which changes the format of the file size returned by the fsize command.

  sizefmt can be “bytes,” which displays the file size in bytes or “abbrev,” which displays the file size in kilobytes (this is the default when the fsize command is used alone).

- timefmt, which sets the format of the last modification date returned by the flastmod command.

  timefmt is expressed using a series of formatting symbols called field descriptors. For example, the field descriptor %D is used to display the date in the MM/DD/YY format and %a is used to display the abbreviated weekday name. For a complete list of field descriptors, consult a good source on Web server administration, such as *Serving the Web* by Robert Jon Mudry (Coriolis Group Books).

- errmsg, which sets the error message returned when the server encounters an SSI error.
- onerr, which indicates what action the server takes when it encounters an SSI error.

  Possible actions are goto (jumps to a specific label command), print (prints specific text), error (prints the current errmsg string), break (terminates the HTML document), errorbreak (prints the current errmsg string and terminates the HTML document), and printbreak (prints specific text and terminates the HTML document).

For example, the following command changes the format of the file size and last modification date so that the file size is displayed in bytes, the date is displayed in the MM/DD/YY format, and the time is displayed in hours, minutes, and seconds AM or PM:

<!--#config sizefmt=“bytes” timefmt=“%D %r”-->

To set the SSI error message to “Sorry, we encountered an error while processing your document” and instruct the server to print this error message when it encounters an SSI error, then terminate the HTML document, type the following commands into the document:

<!--#config errmsg=‘Sorry, we encountered an error while processing your document’-->
<!--#config onerr=“errorbreak”-->

append Command

Use the append command to add information to a text file whenever a user requests a specific HTML document or submits an HTML form.

The append command supports two tags.

- file, which identifies the text file to which the data is appended
- line, which specifies what information is added to the text file

The append command uses the following syntax:

<!--#append file="*filename*" line="*lines*"-->

For example, suppose you have an HTML form that requests information about users wanting to learn more about your products. The form requests the user's last name, first name, address, city, state, zip code, phone number, and fax number. When the user submits the form, you want the information to go into a sales database. To append this information to the file salesdb.txt whenever the form is submitted, type the following command into the HTML form:

<!--#append file="salesdb.txt" line="&&Last&&, &&First&&, &&Addres&&, &&City&&, &&State&&, &&Zip&&, &&Phone&&, &&Fax&&"-->

count Command

Use the count command to display the number of times the current file has been accessed.

The count command supports one tag.

- file, which identifies what file the server will use to track the number of document hits. You can use any valid filename.

This command uses the following syntax:

<!--#count file="*filename*"-->

The following example shows how to use the count command to display the number of hits:

```
<p>
You are number <!--#count file="counter.txt"--> to access this document!
<br>
```

if Command

Use the if command to instruct the server to perform an operation based on the outcome of a logical comparison (for example, *if* this, *then* do this).

The if command uses the following syntax:

<!--#if “*operand1*” *operator* “*operand2*” *operation*-->

operand1 is any string or number to which *operand2* should be compared.

operator is the method that should be used to compare *operand1* and *operand2*. Possible operators are == (equal to), != (not equal to), < (less than), > (greater than), >= (not less than), <= (not greater than), or contains (the text string in operand2 is found in the operand1 string).

operand2 is any string or number to which operand1 should be compared.

operation is the action the server should take when the comparison of operand1 and operand2 is true. Possible operations are

- goto, which instructs the server to jump to a specific label command
- print, which instructs the server to print specific text
- error, which instructs the server to print the current errmsg string
- break, which instructs the server to truncate the HTML document
- errorbreak, which instructs the server to print the current errmsg string and then truncate the HTML document
- printbreak, which instructs the server to print specific text and then truncate the HTML document.

For example, the following if command instructs the server to jump to a specific line if the request came from an NCSA Mosaic browser. If the request did not come from an NCSA Mosaic browser, the server will jump to a different location in the HTML file.

```
<!--#if “&&HTTP_USER_AGENT&&” contains “Mosaic” goto mosaiclabel-->
<p>You are not using Mosaic.
<!--#goto “defaultlabel”-->
<!--#label “mosaiclabel”-->
<p>You are using Mosaic
<!--#label “defaultlabel”-->
```

goto Command

Use the goto command to jump to the point in the HTML document that is identified by a specific label command. When the server encounters a goto command, it jumps to the label command without executing any server-side include (SSI) commands or printing any HTML text between the goto command and the label command.

The goto command uses the following syntax:

<!--#goto “label”-->

For example, when the server encounters the following goto command in an HTML document, it jumps to the jumphere label without printing the line between the goto and label commands:

```
<!--#goto “jumphere”-->
<p>This line will not print.
<!--#label “jumphere”-->
<p>This line will print.
```

label Command

Use the label command to mark the spot in the HTML document to which the server jumps when it encounters a goto command that identifies that label as the target.

The label command uses the following syntax:

<!--#label “*labelname*”-->

labelname is a string of 254 characters or less.

For example, when the server encounters the following goto command in an HTML document, it jumps to the jumphere label without printing the line in between the goto and label commands:

```
<!--#goto “jumphere”-->
<p>This line will not print.
<!--#label “jumphere”-->
<p>This line will print.
```

break command

Use the break command to truncate an HTML document.

The break command uses the following syntax:

<!--#break -->

The following example illustrates the break command:

<p>This line will print.
<!--#break -->
<p>This line will not print because the document has been truncated and transmission to the client is terminated.

calc Command

Use the calc command to perform mathematical calculations.

The calc command uses the following syntax:

<!--#calc *variablename1* = "*value*" -->
<!--#calc *variablename2* = "*value*" -->
<!--#calc *sum* = "*variablename1+variablename2*" -->

The following operands are valid: +, *, -, /. Equations can contain parentheses to prioritize operations.

The following example illustrates the calc command:

```
<p>calc test:<br>
<!--#calc number1="1" -->
<!--#calc number2="2" -->
<!--#calc number3="3" -->
<!--#calc sum="(number1+number2)*number3" -->
The result is <!--#echo format "%8.2f" "sum"-->
```

This example prints the following result:

The result is 9.00

Document Tree

The part of the server's file system that has been set aside for Web documents. Web clients can only access documents that are stored in the document tree. Web clients cannot access other directories in the server's file system.

NDS Browser

An extension NLM* that allows clients to browse the NDS* (Novell Directory Services*) tree using an HTML browser, such as Netscape Navigator**, and view the objects and their attributes within the tree. Object types are represented by icons and object names. Users use their mouse to click on the icons and browse through the tree.

*Novell trademark. ** Third-party trademark. Use Index for trademark information.

Authentication

A means of verifying that the user sending requests to the NetWare* Web Server* is authorized to do so. You can use Novell Directory Services* (NDS*) authentication or you can create your own text-based username and password file to authenticate NetWare Web Server users.

*Novell trademark. ** Third-party trademark. Use Index for trademark information.

How Do I . . .

Configure the server

Manage the document tree

Set up access control

Manage logging

Start and stop services

Remove the software

Find out how to create dynamic Web pages

Configuring the Server

The NetWare* Web Server* comes with a default configuration that enables it to run immediately after installation. Although this default configuration provides you with basic Web server functionality, you will probably want to customize the Web server to fit in your specific environment.

There are two ways to customize the server, depending on your requirements.

- Modify the basic configuration parameters, using the NetWare Web Server administration utility running on a Windows** or Windows 95 workstation.
- Make advanced configuration changes, using any text editor to edit the Web server configuration files.

You can also modify the NetWare server configuration to

- Tune system performance when multiple application NLM* programs are run on the server
- Set up long file name support for Java** applets

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Modifying the Basic Server Parameters

The basic server parameters are all displayed on the Server tab page. Modify the basic server parameters using the NetWare* Web Server* administration tool as follows:

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. If your network uses DNS and the Web server should include hostnames instead of IP addresses in the URLs to which it redirects clients, type the fully qualified DNS name for the server in the Full server name field. If your network does not use DNS, type the server's IP address in the Full server name field. An entry in this field is mandatory.
5. If the server should listen for HTTP requests on a port other than 80, type the port number in the TCP port number field.
6. If you want users to report problems with the Web server by e-mail, type the e-mail address in the Administrator's e-mail address field.
7. If you want to move the document root directory from the default location, type the new path to the directory in the Directory containing HTML documents field.
8. If you want to move the log files from the default location, type the new path to the files in the Directory containing log files field.
9. If you want to allow users to publish their own Web documents from their home directories on the server, check Enable user documents. Then type the name of the subdirectory that should contain the users' documents within their home directories in the User subdirectory field.
10. If you want to allow users to use the NDS browser to browse the NDS* (Novell Directory Services*) tree, check Enable NDS browsing.
11. Click OK.
12. Click Save and Restart.
13. Type the Web server password and click OK.

Setting the Advanced Server Parameters

You can perform the following advanced server configuration tasks by editing the Web server configuration files using any text editor:

Setting up name resolution

Setting the maximum number of threads

Setting the time-out interval

Setting the location of the MIME types file

Setting the location of the server resources map

Setting Up Name Resolution

Every time a client makes a request to the NetWare* Web Server*, the request is logged to the SYS:WEB\LOGS\ACCESS.LOG file. If you want the server to record hostnames rather than IP addresses in the log entries, set up name resolution as follows:

- If your network does not use DNS, add IP-address-to-hostname mappings for each client system to the server's SYS:ETC\HOSTS file.
- If your network uses DNS, make sure there is a valid SYS:ETC\RESOLV.CFG file on the server.

Setting Up the SYS:ETC\HOSTS File

The SYS:ETC\HOSTS file is a database file that contains IP-address-to-hostname mappings for all known hosts on an IP internetwork. If your network does not use DNS and you want the Web server to log hostnames instead of IP addresses to the ACCESS.LOG file, you must create an entry for every known client system in the SYS:ETC\HOSTS file.

The SYS:ETC\HOSTS file uses the same format as the /etc/hosts file on UNIX** systems. Use the following format to add a host entry to the SYS:ETC\HOSTS file:

```
IP_address hostname [alias [ . . .]]
```

For example, to add an entry for a client system with an IP address of 123.45.6.7 with a hostname of john.galaxy.com and an alias of john, you add the following line to the SYS:ETC\HOSTS file:

```
123.45.6.7 john.galaxy.com john
```

Setting Up the SYS:ETC\RESOLV.CFG File

The SYS:ETC\RESOLV.CFG file is a database file that contains the name of the server's DNS domain and the IP address of the DNS name server for the domain. If you use DNS on your network and you want the Web server to log hostnames rather than IP addresses in its ACCESS.LOG file, you need a valid SYS:ETC\RESOLV.CFG file.

The SYS:ETC\RESOLV.CFG file uses the same syntax as the /etc/resolv.conf file on UNIX** systems. If your network uses DNS and the server does not have a SYS:ETC\RESOLV.CFG file, create one using the following syntax:

```
domain domain_name
nameserver IP_address
```

For example, if your NetWare* Web Server* belongs to the sales.galaxy.com DNS domain served by a DNS name server at 123.45.6.8, your SYS:ETC\RESOLV.CFG file would look like the following:

```
domain sales.galaxy.com
nameserver 123.45.6.8
```

Setting the Maximum Number of Threads

Every time a Web client sends a request to the NetWare* Web Server*, the server starts a new process, or thread, to handle the request. This enables the server to handle multiple HTTP requests concurrently. By default, the server starts a maximum of 16 concurrent threads. This default value should be fine for most Web servers. However, you might want to modify the maximum number of threads if

- The server has a large memory pool and is a dedicated Web server handling a high volume of HTTP requests. In this case, you might want to increase the maximum number of threads so that the server can handle more concurrent requests. Keep in mind, however, that each thread requires additional memory.
- The server is low on memory and is not a dedicated Web server. In this case, you might want to reduce the maximum number of threads to free memory for other NetWare services.

To modify the maximum number of threads, edit the \WEB\CONFIG\HTTPD.CFG file as follows:

1. Use any text editor to open the \WEB\CONFIG\HTTPD.CFG file.
2. Add the following line to the file:

   ```
   MaxThreads n
   ```

   where *n* is the maximum number of concurrent threads the Web server can start.
3. Save the file.

Setting the Time-Out Interval

The time-out interval is the maximum time in seconds that the Web server waits for a client system to

- Make a request after the HTTP connection is opened
- Accept the data returned by the Web server in response to a request

The default interval is 60 seconds. You can increase or decrease this value by editing the SYS:WEB\CONFIG\HTTPD.CFG file as follows:

1. Use any text editor to open the SYS:WEB\CONFIG\HTTPD.CFG file.
2. Add the following line to the file:

   ```
   TimeOut time
   ```

   where *time* is the amount of time in seconds the Web server should wait for a client to request or accept data.
3. Save the file.

Setting the Location of the MIME Types File

The Types Configuration file (MIME.TYP) contains a list of MIME types supported by the NetWare* Web Server*. When the HTTP.NLM loads, it must be able to find the MIME.TYP file.

By default, the Web server looks for this file in the \WEB\CONFIG directory. However, if you change the location of the Web server configuration files, the server will not be able to find this file. In this case, modify the TypesConfig directive in the HTTPD.CFG file as follows:

1. Use any text editor to open the SYS:WEB\CONFIG\HTTPD.CFG file.
2. Modify the following line:

   `TypesConfig` *`new_path`*

   where *new_path* is the path of the MIME.TYP file relative to the server root.

3. Save the file.

Setting the Location of the Server Resources Map

The Server Resources Map file (SRM.CFG) controls the location of server resources such as documents and scripts. When the HTTP.NLM loads, it must be able to find the SRM.CFG file. By default, the Web server looks for this file in the \WEB\CONFIG directory. However, if you change the location of the Web server configuration files, the server will not be able to find this file. In this case, modify the ResourceConfig directive in the HTTPD.CFG file as follows:

1. Use any text editor to open the SYS:WEB\CONFIG\HTTPD.CFG file.
2. Modify the following line:

   ```
   ResourceConfig new_path
   ```

   where *new_path* is the path of the SRM.CFG file relative to the server root.
3. Save the file.

Tuning System Performance for Multiple NLM* Programs

The Web server installation adds the following line to the SYS:SYSTEM\AUTOEXEC.NCF file:

```
SET MAXIMUM PACKET RECEIVE BUFFERS=1000
```

This is the optimal setting for the Web server NLM. You might have other NLMs running on your NetWare* server that recommend different settings for optimal performance. When tuning this parameter to support multiple NLMs, use the highest value required by any of the NLMs.

If the existing AUTOEXEC.NCF file contains a SET MAXIMUM PACKET RECEIVE BUFFER=1000 line with extra white spaces, the Web server installation could add the line again. Delete this extra line.

Setting Up Long Name Space Support

Java** applets are usually represented by filenames beyond the DOS 8.3 convention and must be stored on a disk volume that supports long filenames. The NetWare* long name space module (LONG.NAM) can be used to provide long filename support for Java applets. This module is installed in the SYS:SYSTEM directory during the standard NetWare* installation.

Each name space added to a volume requires additional server memory. If you add name space support to a volume and do not have enough memory, that volume cannot be mounted. Use the following formula to calculate the additional memory required for each name space added to a volume:

0.032 x *volume_size* (in MB) /*block_size* (in KB)

Round the result to the nearest megabyte and verify that the memory is available.

For example, adding a long name space to a 100-MB volume with a block size of 4 KB would require 1 MB (0.032 x100 MB/4=0.8 MB) of additional memory.

After verifying that memory is available, set up long name space support as follows:

1. Verify that the LONG.NAM module exists in the SYS:SYSTEM directory where NetWare is installed.
2. At the server console prompt, type

   LOAD LONG.NAM <Enter>
   ADD NAME SPACE LONG TO *volume_name*

   where *volume_name* is the volume to which to add long name space support.
3. Type the following at the server console to verify that the long name space has been added:

   VOLUMES <Enter>

After you have added a name space, the module autoloads each time the server comes up. As a result, you need to add the name space to a volume only once.

Managing the Document Tree

The directory structure that contains the documents you publish on the Web server is called the document tree. At the top of the document tree is the document root. Web clients can access any file located in the document root directory or any of its subdirectories; Web clients cannot access any files located above the document root directory.

You can perform basic document tree management tasks using the NetWare* Web Server* administration utility.

You can perform advanced document tree management tasks by editing the Web server configuration files.

Setting Up a Basic Document Tree

Publishing documents on the Web server is simple. All you have to do is store your files in the appropriate directories in the document tree. The NetWare* Web Server* includes a default document tree that you can use to publish documents immediately.

To customize the default document tree you can

Move the document root

Set up a new directory

Remove a directory

Set up directory indexing

Set up server-side includes

Set up support for user directories

Set up a home page

Publishing Documents on the Default Document Tree

The NetWare* Web Server* includes a default document tree. To publish your documents using this document tree, store the files as follows:

- Store HTML documents in the SYS:WEB\DOCS directory.
- Store server-side include documents (.SSI files) in the SYS:WEB\DOCS\SSI directory.
- Store graphics files (.GIF or .JPG files) in the SYS:WEB\DOCS\IMAGES directory.
- Store image map configuration files in the SYS:WEB\DOCS\MAPS directory (the actual image map graphics file goes in the SYS:WEB\DOCS\IMAGES directory).
- Store BASIC RCGI scripts in the SYS:WEB\SCRIPTS directory.
- Store NetBasic scripts in the SYS:NETBASIC\WEB directory.
- Store Perl RCGI scripts in the SYS:WEB\SCRIPTS\PERL directory.
- Store LCGI NLM* extension programs in the SYS:WEB\LCGI directory.

You can store documents, image files, and NLM* programs in any directory under the \DOCS directory. However, store image map configuration files and scripts only in the specified directories.

Moving the Document Root

The document root is the top of your document tree. The documents you publish on the Web server must be stored in the document root directory or one of its subdirectories.

The document root directory is also the directory where the server's home page file is stored. By default, the document root is set to the SYS:WEB\DOCS directory.

If you want to move the document root directory, use the following procedure:

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the Web server and click OK.
4. Type the new path to the document root in the Directory containing HTML documents field.
5. Click OK.
6. Click Save and Restart.
7. Type the Web server password and click OK.

Setting Up a New Directory

You can add a new directory to the document tree by creating a new directory under the document root. The document and image files you store in the new directory can be accessed by Web clients immediately.

When you add a new directory this way, the new directory inherits the directory options and access control settings of the parent directory. If you want the new directory to have different directory options or access control settings, add an entry for the directory as follows:

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Select the Directories tab.
5. Type the path to the new directory in the Directory path field or browse for the path by clicking Browse.
6. Indicate what type of files the new directory contains by selecting a file type from the Contains drop-down list.
7. Set up any special features for the new directory as follows:

   To enable automatic indexing for the directory, check Enable indexing in the Features box. If you enable indexing, indicate whether you want to use fancy indexing, icons are links, or scannable titles by checking the appropriate options in the Index options box.

   To enable server-side includes in the directory, check Enable includes in the Features box.
8. Click Add.
9. Click OK.
10. Click Save and Restart.
11. Type the Web server password and click OK.

After you finish adding the new directory, you can restrict access to the directory by authorized system or user.

Removing a Directory from the Document Tree

To remove a directory from the document tree

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Select the Directories tab.
5. Select the directory you want to remove from the Existing directories list.
6. Click Remove.
7. Click OK.
8. Click Save and Restart.
9. Type the Web server password and click OK.
10. Delete the directory and its contents from the server's file system.

Setting Up Directory Indexing

A directory index is a document that describes the contents of a directory on the Web server. There are two ways to provide directory indexes.

- You can create an HTML document called INDEX.HTM that describes the contents of the directory. (A home page is an example of a directory index that you create.) When a user types in the URL of a directory rather than a file, the Web server automatically looks for an INDEX.HTM file to return.
- You can set up the Web server to generate an index automatically whenever a user types in the URL of the directory. This is useful when the contents of a directory change often or when a directory contains many files. If the directory does not contain an INDEX.HTM file and automatic directory indexing is not enabled, the Web server returns an error code.

To set up automatic directory indexing

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Select the Directories tab.
5. Select the directory in which you want to enable automatic directory indexing from the Existing directories list.
6. Check Enable indexing.
7. Set the Index options as follows:

   If you want the index entries to include icons, file size information, and descriptions in addition to filenames, check Fancy indexing.

   If you want users to be able to click on icons to retrieve an associated file, check Icons are links.

   If you want the Web server to generate a description for each file by scanning the HTML documents for titles, check Scan titles.
8. Click OK.
9. Click Save and Restart.
10. Type the Web server password and click OK.

Setting Up Server-Side Includes

The server-side include (SSI) mechanism enables the Web server to modify HTML documents slightly before sending them to a requesting client. The changes the Web server makes are controlled by SSI commands that you embed into the HTML document.

To set up server-side includes, you must

- Enable the server-side include mechanism for a directory
- Create server-side include documents

Creating Server-Side Include Documents

A server-side include (SSI) document is any HTML document that contains embedded SSI commands. All SSI documents must use the .SSI filename extension and must be stored in a directory in which SSI has been enabled. The default directory in which to store SSI documents is SYS:WEB\DOCS\SSI.

To include an SSI command in an HTML document, you simply type the command into the document at the point where you want the server to execute the command. All SSI commands are case-sensitive and use the following general syntax:

<!--#command tag="value"-->

The NetWare* Web Server* supports the following SSI commands:

- The include command instructs the Web server to append a specified file to the document.
- The echo command instructs the Web server to display information defined by a set of environment variables in the document.
- The flastmod command instructs the Web server to display the date on which a specific file was last modified in the document.
- The fsize command instructs the Web server to display the size of the file or another file in the document.
- The config command instructs the Web server how to display the last modified date or the file size information. This command is used with the flastmod command or the fsize command.
- The append command instructs the Web server to append information to a specific text file.
- The count command instructs the Web server to print the number of times the document has been accessed.
- The if command instructs the Web server to perform an operation based on a condition.
- The goto command instructs the Web server to jump to a specific location in the document.
- The label command identifies the location to which an if...goto command or a goto command jumps.
- The break command truncates the document.
- The calc command performs mathematical calculations.

Enabling Server-Side Includes

To enable server-side includes (SSIs) for a specific directory

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Select the Directories tab.
5. Select the directory in which you want to enable SSIs from the Existing directories list.
6. Check Enable includes.
7. Click Change.
8. Click OK.
9. Click Save and Restart.

Setting Up Support for User Directories

In addition to publishing documents from the document tree, users at your site can publish their own documents from their home directories. To enable support for user directories

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Check Enable user documents.
5. Type the name of the subdirectory in the users’ home directory in which users' Web documents will be stored.
6. Click OK.
7. Click Save and Restart.
8. Type the Web server password and click OK.

Enabling NDS Browsing

An extension NLM* allows clients to browse the NDS* (Novell Directory Services*) tree using an HTML browser, like Netscape Navigator**, and view the objects and their attributes within the tree. Object types are represented by an icon and the object name.

The NDS browser is disabled by default. You should enable the NDS browser only if you want external users from the Internet to read public information stored in your NDS trees. You can limit the amount of information that is visible from the NDS browser. For example, if you would like only the e-mail address property visible, set up the [PUBLIC] trustee to only have read rights to this property of user objects.

To enable the NDS browser

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Check Enable NDS browsing.
5. Click OK.
6. Click Save and Restart.
7. Type the Web server password and click OK.

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Setting Up a Home Page

A home page is usually the first document returned when a Web client connects to your server. A good home page contains a high-level overview of the information available at your site and includes links to other documents.

The NetWare* Web Server* includes a default Novell* NetWare Web Server home page. This home page (SYS:WEB\DOCS\INDEX.HTM) contains important information about the server and provides links to example HTML files, image maps, BASIC and Perl scripts, and NLM* programs for you to try out. After you are familiar with the capabilities of the server, you might want to create your own home page.

To set up your own home page

1. Store the HTML file for your home page in the SYS:WEB\DOCS directory as INDEX.HTM.
2. Store all supporting graphics and image map files in the appropriate directories on your document tree.

Setting Advanced Document Tree Features

You can perform the following advanced document tree setup tasks by editing the NetWare* Web Server* configuration files:

Set up image map support

Add support for new document types

Set the default document type

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Setting Up Image Map Support

An image map is a graphics file that contains active areas called hotspots. When a user clicks on a hotspot, the server interprets the coordinates on which the user clicked and then refers to an image map configuration file. The file defines what action the server takes. For example, the image map configuration file might instruct the server to return a different URL or to run an RCGI extension script or program.

To set up support for image maps

1. Create the image map graphics file and store it in the document tree (for example, in the \WEB\DOCS\IMAGES directory).
2. Create an image map configuration file defining the hotspots and the server actions and store it in the \WEB\MAPS directory.
3. Reference the image map in an HTML document using the ISMAP HTML tag.

The NetWare* Web Server* supports the NCSA format for image map configuration files. For more information on setting up image map support, consult a good source on Web server administration, such as *Serving the Web* by Robert Jon Mudry (Coriolis Group Books).

Adding Support for a New Document Type

Every document served by the Web server is assigned a Multimedia Internet Mail Extensions (MIME) type header that describes the content of the document and maps a file extension to a type of data. For example, an HTML file is assigned the MIME type of text /html. Every document retrieved from a Web server contains a MIME type header that tells the browser what to do with the file.

The MIME types supported by the NetWare* Web Server* are stored in the SYS:WEB\CONFIG\MIME.TYP file. If you want to add support for a new document type, you must add a line to the MIME.TYP file, as follows:

1. Use any text editor to open the SYS:WEB\CONFIG\MIME.TYP file.
2. Add an entry for the new file type using the following syntax:

   ```
   type/subtype extension
   ```

   type is a data type such as text, application, image, or video.

   subtype is a more specific description of the data type. For example, html, plain, and richtext are subtypes of the type text data. The subtypes you add must begin with an x-. For example, to add a MIME type mapping for WordPerfect documents, you might use the subtype x-wordperfect.

   extension is the file extension that maps to the MIME type. For example, the extension txt maps all files ending in .txt to the text/plain MIME type.
3. Save the file.

Setting the Default Document Type

Every document served by the Web server is assigned a Multimedia Internet Mail Extensions (MIME) type header that describes the content of the document and maps a file extension to a type of data. For example, an HTML file is assigned the MIME type of text /html. Every document retrieved from a Web server contains a MIME type header that tells the browser what to do with the file.

Make sure you have MIME type entries set up for every type of document you plan to publish on your Web server in the SYS:WEB\CONFIG\MIME.TYP file. You can set up a default MIME type by editing the SYS:WEB\CONFIG\SRM.CFG file as follows:

1. Use any text editor to open the SYS:WEB\CONFIG\SRM.CFG file.
2. Add the following line to the file:

   ```
   DefaultType type/subtype
   ```

   type is a data type such as text, application, image, or video.

   subtype is a more specific description of the data type. For example, html, plain, and richtext are subtypes of the *type* text data.
3. Save the file.

Setting Up Access Control

By default, anyone can access the NetWare* Web Server*. However, you can control who accesses the directories in your document tree. There are two ways to control access.

- You can control access to any directory in the document tree from a central file called the global access control file (SYS:WEB\CONFIG\ACCESS.CFG). You can add access control entries to the global access control file using the NetWare Web Server administration utility.
- You can decentralize the administration of access control to the directories in the document tree by allowing access control entries to be added to a per-directory access control file. A per-directory access control file contains access control entries for the directory in which the file resides and its subdirectories. Per-directory access control files must be created manually.

By default, per-directory access control is enabled for all directories in the document tree. However, you can disable per-directory access control for any directory in the document tree except the document root directory.

Setting Up Global Access Control

The global access control file (\WEB\CONFIG\ACCESS.CFG) controls access to any directory in the document tree. You can restrict access to the directories in the document tree by

- Authorized system
- Authenticated user

You must use the NetWare* Web Server* administration utility to set up the global access control file.

Restricting Directory Access by Authenticated User

The NetWare* Web Server* enables you to authenticate Web users using either of the following authentication methods:

- Novell Directory Services* (NDS*) authentication
- File-based authentication

NDS authentication must be set up globally (in the \WEB\CONFIG\ACCESS.CFG file). File-based authentication must be set up by directory (in the ACCESS.CFG file that resides in the directory). You can only use one authentication method for any given directory.

NDS Authentication

When a Web client requests a document that resides in a directory in which NDS authentication controls access, the Web server prompts for a username and password. After the user enters an NDS username and password, the NetWare Web Server checks the NDS database to ensure that the username and password are correct before returning the document.

You must use the NetWare Web Server administration utility to set up NDS authentication.

File-based Authentication

When a Web client requests a document that resides in a directory in which file-based authentication is used to control access, the Web server prompts for a username and password. After the user enters a Web server username and password, the NetWare Web Server checks its user database file to ensure that the username and password are correct before returning the document.

You must manually edit the per-directory access control file to set up file-based authentication.

Setting Up Per-Directory Access Control

The per-directory access control file (ACCESS.WWW) controls access to the current directory only. For example, the ACCESS.WWW file that resides in the /DOCS/MOREDOCS directory restricts access to documents in the /DOCS/MOREDOCS directory only.

You can manually create the ACCESS.WWW files using any text editor. A per-directory access control file can restrict access to the directories in the document tree by

- Authorized system
- Authenticated user

Restricting Directory Access Using NDS* Authentication

If you are setting up NDS-based authentication for a directory by editing the per-directory access control file that resides in the directory (ACCESS.WWW), you must add the AuthType, AuthName, and AuthUserMethod directives before the <Limit GET> directives.

For example, to set up the \WEB\DOCS directory so that it authenticates users based on their NDS usernames and passwords, edit the \DOCS\ACCESS.WWW file as follows:

```
AuthType Basic
AuthName NDS
AuthUserMethod nds nds_context
<Limit GET>
require valid_nds_user
</Limit>
```

In this example, *nds_context* is the NDS context in which the user objects you want to allow access to the directory reside, and v*alid_nds_user* is any user listed in the NDS database.

Using the Access Control File to Restrict Access by System

You can restrict directory access to authorized systems by full IP address, partial IP address, DNS domain name, or DNS hostname. Enter the access control directives into the ACCESS.WWW file that is stored in the directory you want to restrict.

Restricting Access by Full IP Address

These ACCESS.WWW entries grant access to the current directory only to the system with the IP address 123.45.6.7.

```
<Limit GET>
order deny,allow
deny from all
allow from 123.45.6.7
</Limit>
```

Restricting Access by Partial IP Address

These ACCESS.WWW entries grant access to the current directory only to the systems in the 123.45.6.0 subnetwork.

```
<Limit GET>
order deny,allow
deny from all
allow from 123.45.6
</Limit>
```

Restricting Access by DNS Domain

These ACCESS.WWW entries grant access to the current directory only to the systems in the marketing.yourcompany.com DNS domain.

```
<Limit GET>
order deny,allow
deny from all
allow from marketing.yourcompany.com
</Limit>
```

Restricting Access by DNS Hostname

These ACCESS.WWW entries grant access to the current directory only to the host named host1 in the marketing.yourcompany.com domain.

```
<Limit GET>
order deny,allow
deny from all
allow from host1.marketing.yourcompany.com
</Limit>
```

For more detailed information on setting up access control and other directory features, refer to one of the following sources:

- A good text on Web server administration, such as *Managing INTERNET Information Services* by Liu, Peek, Jones, Buus, and Nye (O'Reilly & Associates, Inc.)
- http://hoohoo.ncsa.uiuc.edu/docs/setup/access/Overview.html
- http://hoohoo.ncsa.uiuc.edu/docs/tutorials/user.html

Restricting Directory Access Using File-Based Authentication

There are two steps required to set up file-based authentication for a directory.

1. Create a users database file
2. Edit the ACCESS.WWW file

Creating the Users Database File

When you use file-based authentication, you must manually create a users database file that lists all users and their corresponding clear-text passwords. You then run the SYS:PUBLIC\PWGEN.EXE program to create a new file containing a list of users and their corresponding encrypted passwords.

To create the users database file

1. Use any text editor to create a text file listing all the users you want to authenticate and their corresponding clear-text passwords. For example, create a file called users.txt using the following syntax:

   user1:password1
   user2:password2

2. Map a drive to the SYS:PUBLIC directory on the NetWare* Web Server*.

3. Type the following command at the DOS prompt:

   `x:pwgen` *`file1 file2`* `<Enter>`

   where *x* is the drive letter that is mapped to the server's SYS:PUBLIC directory, *file1* is the pathname and filename (relative to the server root) of the user database file you created, and *file2* is the pathname and filename (relative to the server root) of the new file.

4. Store the encrypted user database file (file2) in the server root directory (SYS:WEB by default).

Editing the ACCESS.WWW file

To restrict directory access using file-based authentication, manually edit the per-directory access control file (the ACCESS.WWW file located in the directory you want to restrict) to add the following directives before the <Limit GET> directive:

AuthType Basic
AuthName *name*
AuthUserFile *filename*

where *name* is any name that identifies to the user which username and password to enter and *filename* is the name of the user database file generated by the pwgen program. The filename you specify must be relative to the server root directory.

For example, suppose you want to restrict access to the \DOCS\MOREDOCS directory so that only user landrew listed in a user database file called SYS:WEB\HTPASSWD.WWW is allowed to access documents in the directory. When a client requests a document in the \DOCS\MOREDOCS directory, the browser prompts for the Web username and password. In this case, you would create a \DOCS\MOREDOCS\ACCESS.WWW file containing the following lines:

```
AuthType Basic
AuthName Web
AuthUserFile htpasswd.www
<Limit GET>
require user landrew
</Limit>
```

Or, to allow all users listed in the SYS:WEB\HTPASSWD.WWW file to access the \DOCS\MOREDOCS directory, you would use the keyword valid-user in the <Limit GET> directive in the \DOCS\MOREDOCS\ACCESS.WWW file.

```
AuthType Basic
AuthName Web
AuthUserFile htpasswd.www
<Limit GET>
require valid-user
</Limit>
```

Disabling Per-Directory Access Control

To disable per-directory access control for a given directory, edit the corresponding access control entry in the global access control file as follows:

1. Use any text editor to open the SYS:WEB\CONFIG\ACCESS.CFG file.
2. Locate the directory entry that corresponds to the parent directory of the directory in which you want to disable per-directory access control. This entry is delimited by a <Directory *directory_name*> entry.
3. Edit the AllowOverride directive to read

   AllowOverride none

4. Save the file.

Using the Utility to Restrict Access by System

When you restrict directory access to authorized systems, the Web server checks the Web client's IP address or DNS domain name before fulfilling a document request. You can restrict directory access to authorized systems

- By full IP address.

  For example, if you restrict directory access to 123.45.6.7, only the system with that IP address will be able to access documents in the directory.

- By partial IP address.

  For example, if you restrict directory access to 123.45.6, only the systems in the 123.45.6.0 subnet will be able to access documents in the directory.

- By DNS domain name.

  For example, if you restrict directory access to the yourcompany.com domain, only systems in that domain will be able to access documents in the directory.

To restrict directory access to authorized systems

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Select the System Access tab.
5. Select the directory you want to control from the Directory drop-down list.
6. Type the full or partial IP address or the fully qualified DNS domain name or hostname in the appropriate field.
7. Click Add to Authorized systems list.
8. Repeat steps 6 and 7 for each authorized system or group of systems.
9. Click OK.
10. Click Save and Restart.
11. Type the Web server password and click OK.

Restricting Directory Access Using NDS Authentication

When you restrict directory access to authorized users or groups, the Web server checks the Web client's NetWare* username before fulfilling a document request. You can restrict directory access to authorized users by Novell Directory Services* (NDS*) user or group object.

To restrict directory access to authorized NDS users or groups

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Select the User Access tab.
5. Select the directory you want to control from the Directory drop-down list.
6. Select Directory Services from the Authentication method drop-down list.
7. Type the name of the NDS context that contains the user or group object you want to allow to access the directory in the Browse network users field.
8. Select an authorized user or group from the Network users list.
9. Click Add to Authorized users list.
10. Repeat Steps 8 and 9 for each authorized user or group.
11. Click OK.
12. Click Save and Restart.
13. Type the Web server password and click OK.

Managing Logging

The NetWare* Web Server* generates three log files.

- The Access Log, which lists every request made to the server. This log file uses the common log format to record the username of the user who made the request, whether the user was authenticated, the date and time of the request, the actual request, the status code, and the number of bytes sent.
- The Error Log, which lists error conditions such as client time-outs, script errors, user authentication configuration errors, and server errors.
- The Debug Log, which lists diagnostic information that can be used to troubleshoot the Web server.

The NetWare Web Server writes to these files every 3 minutes.

You can perform the following log file management tasks using the NetWare Web Server administration utility:

Move the location of the log files

Set the logging parameters

View the access log

View the error log

View the debug log

Clear a log file

Print a log file

Copy data from a log file

Save a log file

Moving the Location of the Log Files

By default, the log files are stored in the SYS:WEB\LOGS directory. If you want to move the log files to a new directory, use the following procedure:

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Type the new path to the log files in the Directory containing log files field.
5. Click OK.
6. Click Save and Restart.
7. Type the Web server password and click OK.

Setting the Logging Parameters

The logging parameters control the size of the log files and the level of logging. These parameters also control whether the server will roll the log files when they reach a maximum size. To roll a log file, the server saves the file under a new name and opens a new file in which to resume logging. For example, when the ACCESS.LOG file reaches its maximum size, the server saves it to ACCESS.1 and opens a new ACCESS.LOG file. If the server is not set up to roll the log files, the log files will continue to grow until you clear them manually.

To set the log file parameters

1. Click File.
2. Click Select Server.
3. Select the \WEB directory on the drive that is mapped to the server and click OK.
4. Select the Logs tab.
5. If you want the server to roll the log files

   a. Check Roll logs as needed from the Log file handling box.

   b. Type the file size in KB after which the server should roll the log files in the Maximum log size field.

   c. Type the maximum number of old log files the server should store in the Max. number of old logs field.
6. Indicate whether you want the server to generate a debug log.
7. If you want the server to generate a debug log file, check Log debug information.
8. If you do not want the server to generate a debug log file, check No debug logging.
9. Click OK.
10. Click Save and Restart.
11. Type the Web server password and click OK.

Viewing the Access Log

The Access Log contains an entry for every client request made to the Web server. To view the Access Log file

1. Click Log.
2. Click Open Access.

Viewing the Error Log

The Error Log lists all error conditions encountered on the Web server. To view the Error Log file

1. Click Log.
2. Click Open Error.

Viewing the Debug Log

The Debug Log lists diagnostic information that you can use to troubleshoot the Web server. To view the Debug Log file

1. Click Log.
2. Click Open Debug.

Clearing a Log File

Clearing a log file deletes all data from the file. To clear a log file

1. Open the log file you want to clear.
2. Click Log.
3. Click Clear Log.

Printing a Log File

To print a log file

1. Open the log file you want to print.
2. Click File.
3. Click Print.
4. Click OK.

Copying Data from a Log File

You can copy data from a log file for use in other applications. To copy data from a log file

1. Open the log file.
2. Highlight the text you want to copy.
3. Click Edit.
4. Click Copy.

Saving a Log File

To save a log file to a new file

1. Open the log file.
2. Click Log.
3. Click Save Log As.
4. Type a new name for the file in the File Name field.
5. Click OK.

Starting and Stopping Services

When you change one of the Web server configuration files, the change does not take effect until you stop and restart the Web server. When you use the NetWare* Web Server* administration utility to change the configuration, the utility automatically prompts you to restart the server when you save a change. To restart the server, you must enter a password.

If you make a configuration change manually by editing one of the Web server configuration files, you can either restart the server from the server console prompt or from the administration utility.

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Changing Your Password

The NetWare* Web Server* administration utility requires a password when you save configuration changes and restart the Web server. To change your password

1. Click Server.
2. Click Change Password.
3. Type your current password in the Old password field.
4. Type your new password in the New password field.
5. Retype your new password in the Confirm new password field.
6. Click OK.
7. To restart the Web server, click OK.

Restarting the Web Server from the Server Console Prompt

When you make a Web server configuration change, the change does not take effect until you restart the Web server.

If you have not moved the server root from the default location (SYS:WEB), you can restart the Web server from the server console prompt by typing

unistop <Enter>

unistart <Enter>

If you have moved the server root from the default location, use a text editor to edit the lines in the SYS:SYSTEM\UNISTART.NCF file that load the HTTP and BASIC NLM* programs before you execute the unistop and unistart commands. Edit the lines to read

load http.nlm -d *vol*:*pathname*

load basic.nlm -d *vol*:*pathname*

where *vol:* is the volume containing the Web server root directory and *pathname* is the path to the server root directory.

Restarting the Web Server from the Administration Utility

When you make a Web server configuration change, the change does not take effect until you restart the Web server. To reload the NLM* programs from the NetWare* Web Server* administration utility

1. Click Server.
2. Click Reload.
3. Type your password.
4. Click OK.

Removing the NetWare* Web Server* Software

Use the following procedure to remove the NetWare Web Server software from your NetWare server:

1. Stop the Web server NLM* programs by typing the following command at the server console prompt:

   UNISTOP <Enter>

2. Start the NetWare INSTALL utility from the console prompt by typing

   LOAD INSTALL <Enter>

3. Select Product options.
4. Select View/Configure/Remove installed products.
5. Highlight the NetWare Web Server product entry and press <Delete>.
6. To remove the NetWare Web Server product, select Yes.
7. Press <Esc> three times to exit the installation utility.
8. Select Yes to return to the server console prompt.

Accessing the Dynamic Web Page Programmer's Guide

Remote Common Gateway Interface (RCGI) and Local Common Gateway Interface (LCGI) are the interfaces that allow you to publish dynamic Web pages on the NetWare* Web Server*. To find out how to create your own RCGI scripts or LCGI NLM* extension programs, read the *Dynamic Web Page Programmer's Guide*. View this HTML document using a WWW browser. There are two ways to access this guide:

- You can view the guide installed on your Web Server.
- You can view the guide from the CD.

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Viewing the Dynamic Web Page Programmer's Guide from the CD

To view the *Dynamic Web Page Programmer's Guide* from the CD, you must have a WWW browser. To view the guide

1. Start the WWW browser program from a client workstation.

2. Connect to file:///*cd_drive*:/products/webserv/disk1/web/docs/online/wpguide/ replacing *cd_drive* with the drive letter for the CD-ROM.

Viewing the Dynamic Web Page Programmer's Guide from the Web Server

To view the *Dynamic Web Page Programmer's Guide* installed on the NetWare* Web Server*, you must have a WWW browser. To view the guide

1. Start the WWW browser program from a client workstation.
2. Connect to http://*ip_address*/online/wpguide/ replacing *ip_address* with the IP address of the Web Server.

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Windows

The NetWare* Web Server* administration utility contains the following windows:

- Main Window
- Server tab page
- Directories tab page
- User Access tab page
- System Access tab page
- Logs tab page
- Change Server Password dialog box
- Restart Required dialog box
- Choose a Directory dialog box
- Select Server Root Directory on Web Server dialog box

Using the Main Window

The Main Window is the first window that appears when you start the NetWare* Web Server* administration utility. This window contains the main menu. The main menu provides the following menu options:

- File, which enables you to open a Web server profile for configuration, print a log file, or exit the NetWare Web Server administration utility
- Edit, which enables you to copy text from an open log file
- Server, which enables you to restart the Web server, pause and restart the Web server, or change the Web server password
- Log, which enables you to view the Access, Error, and Debug log files, clear an open log file, or save an open log file to a new filename
- Window, which enables you to perform standard Window operations
- Help, which enables you to access the online help system

You begin all tasks from the main window.

Using the Server Tab Page

Use the Server tab page to modify the basic server configuration parameters. This tab page contains the following fields:

- The Full server name field, which requires the fully qualified name or the IP address of the Web server. If you enter a server name, it must be a valid DNS name (for example, www.yourcompany.com). If you do not use DNS on your network, you must enter the server's IP address. An entry in this field is mandatory.
- The TCP port field, which identifies the TCP port on which the Web server will listen for incoming HTTP requests. You need to modify this value only if your server is listening on a port other than 80 (the default).
- The Administrator's e-mail address field, which contains an e-mail address for the Webmaster. You need to fill in this field only if you want to provide an e-mail address to which users can send comments about or report problems with your Web server.
- The Directory containing HTML documents field, which identifies the document root directory. This can be a full path or the path relative to the server root. You need to modify this field only if you move the document root from the default SYS:WEB\DOCS directory.
- The Directory containing log files field, which identifies the directory in which the Web server creates the Access, Error, and Debug logs. This can be a full path or a path relative to the server root. You need to modify this field only if you want the log files written to a different location.
- The Enable user documents check box, which indicates whether users can publish Web documents from their home directories on the server. Uncheck this check box if you do not want users to publish documents from their home directories.
- The User subdirectory field, which specifies the name of the subdirectory within the users' home directories where users should store documents to be published on the Web. You need to modify this field only if user documents are enabled and you want users to store their Web documents in a subdirectory other than public.www (the default).
- The Enable NDS browsing check box, which indicates whether users can use the NDS browser to browse the NDS* (Novell Directory Services*) tree. Uncheck this box if you do not want users to browse the NDS tree.

You can perform the following tasks from the Server tab page:

- Modify the basic server parameters
- Move the document root directory
- Set up support for user directories
- Move the location of the log files
- Enable NDS browsing

Using the Directories Tab Page

Use the Directories tab page to set up a new directory in the document tree. You can add a new directory to the document tree simply by creating a new directory under the document root. The document and image files you store in the new directory can be accessed by Web clients immediately. However, the new directory inherits its directory options and access control settings from the parent directory. If you want to change the directory options and access control settings, you must first add the new directory using the Directories tab page.

This tab page contains the following fields:

- The Existing directories list, which contains a list of the directories in the document tree.
- The Directory path field, which contains the path to the selected directory or to the directory you are adding to or deleting from the document tree.
- The Contains field, which describes the contents of the selected directory. This field includes a drop-down list for you to choose from. You must fill in the Contains field when adding a new directory to the document tree.
- The Features box, which contains check boxes for enabling automatic directory indexing and server-side includes for the selected directory.
- The Index options box, which contains check boxes for enabling automatic directory indexing options. These options are available only if automatic directory indexing is enabled for the selected directory.

You can perform the following tasks from this tab page:

- Set up a new directory
- Remove a directory
- Set up automatic directory indexing
- Enable server-side includes

Using the User Access Tab Page

Use the User Access tab page to restrict directory access to authorized users.

This tab page contains the following fields:

- The Directory field, which contains a drop-down list of all the directories for which you can set up access control.
- The Authentication method field, which describes the type of authentication used to restrict users and groups. You can choose an authentication method from the drop-down list (Novell* Directory Services* (NDS) is the default).
- The NDS context field, which defines the default NDS* context for users and groups. Users and groups in the default NDS context do not need to provide a full context name when prompted for a username and password.
- The Browse network users field, which you specify the NDS context used to display eligible users and groups in the Network users list.
- The Network users list, which lists all the users and groups you can allow to access the selected directory using the selected authentication method.
- The Authorized users list, which lists all users and groups who currently have access to the selected directory. You can add users or groups to this list by selecting an entry from the Network users list and clicking Add to Authorized users list. You can remove users or groups from this list by selecting the entry you want to remove and clicking Remove.
- The All valid users check box, which allows all users who can be authenticated to have access to the selected directory. When this box is checked, the Network users list is disabled and you cannot select individual users from the Network users list. Uncheck this box to allow individual users.

You can perform the following task using this tab page:

- Restrict directory access to authorized users

Using the System Access Tab Page

Use the System Access tab page to restrict directory access to authorized systems.

This tab page contains the following fields:

- The Directory field, which contains a drop-down list of all directories for which you can set up access control.
- The Full/partial IP address or Domain name field, which identifies the systems to which you want to allow directory access. This field requires either the full or partial IP address or the fully qualified DNS domain name or hostname of the systems you want to be able to access the selected directory.
- The Authorized systems list, which lists all IP addresses or domains that currently have access to the selected directory. You can add entries to this list by typing an IP address or domain name in the appropriate field and then clicking Add to Authorized systems list. You can remove entries from this list by selecting the entry you want to remove and clicking Remove.

You can perform the following task using this tab page:

- Restrict directory access to authorized systems

Using the Logs Tab Page

Use the Logs tab page to manage logging.

This tab page contains the following fields:

- The Log file handling box, which contains option buttons that indicate whether the Web server starts a new log file when a given log file reaches its maximum size. For example, when the ACCESS.LOG file reaches its maximum size, the server saves the file to ACCESS.1 and then opens a new ACCESS.LOG file. If you choose not to roll the log files, the server keeps adding to the log files until you manually clear them.
- The Server debug log options box, which contains option buttons that indicate whether the Web server generates a Debug Log.
- The Maximum log size field, which sets the maximum size of the log files in kilobytes. You can set the value of this field if the Web server is set up to roll the log files. If you set a maximum log file size, the server closes a log file when it reaches the maximum and resumes logging in a new file.
- The Max. number of old logs field, which sets the number of old log files the server stores. You can set the value of this field if the Web server is set up to roll logs. When the /LOGS directory contains the maximum number of old log files, the server deletes the oldest log file before opening a new one.

Using the Change Server Password Dialog Box

Use the Change Server Password dialog box to change the Web server administration password. The Web server requires you to enter this password whenever you save a configuration change or restart the Web server.

This dialog box contains the following fields:

- The Old password field, in which you type your current Web server administration password
- The New password field, in which you type your new password
- The Confirm new password field, in which you retype your new password

You can perform the following task from the Change Server Password dialog box:

- Change the Web server password

Using the Restart Required Dialog Box

Use the Restart Required dialog box to save the Web server configuration files and restart the Web server. Whenever you make a configuration change, you must restart the Web server for the change to take effect.

You can perform the following task from the Restart Required dialog box:

- Restart the Web server from the administration utility

Selecting a Directory

Use this dialog box to select a directory on the NetWare* Web Server*. You can find and select directories using the Drives and Directories lists. If you do not have a drive mapped to the NetWare Web Server, click the Network button to display the NetWare Drive Connections dialog box.

The function of this dialog box depends on the task you are performing.

- If you are selecting a Web server to configure, you must select the server root directory (SYS:WEB by default) on the NetWare Web Server you want to administer in the current session.
- If you are setting up a new directory, modifying the basic server parameters, moving the document root, or moving the location of the log files use this dialog box to select the appropriate directory.

*Novell trademark. ** Third-party trademark. Use Search for trademark information.

Trademarks

Novell and NetWare are registered trademarks and NDS, NetWare Loadable Module, NetWare SFT III, NetWare Web Server, NLM, and Novell Directory Services are trademarks of Novell, Inc.

Java is a trademark of Sun Microsystems, Inc.

Netscape Navigator is a trademark of Netscape Communications Corporation.

Windows is a registered trademark of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.