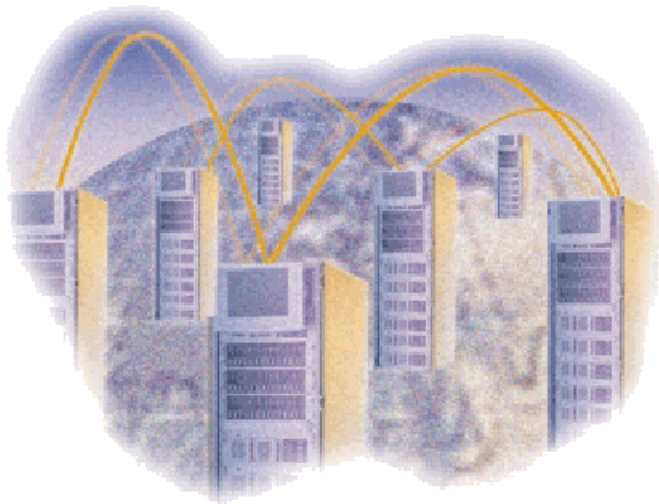




High Availability for Internet Information Server Using Double-Take 4.x



High Availability for Internet Information Server Using Double-Take 4.x published December 2002

NSI and Double-Take are registered trademarks of Network Specialists Inc. All other products are trademarks of their respective companies. © 1996–2002 NSI Software

Double-Take Support for Application Failover

Double-Take's file system replication process is application independent and replicates any file system changes (including permissions and attributes) written to NTFS, FAT or FAT32 file systems by any application or process, subject to specific exceptions called out in the *User's Guide* or *readme.txt* file. Maintaining point-in-time consistent file system replicas and providing server monitoring and automatic or manual failover of the server name and IP address are the primary functions of the Double-Take software and we offer support to qualified customers should these functions fail to operate in accordance with our published documentation, regardless of what application or process is manipulating the data.

NSI Software may provide application notes and other documents that provide implementation guidelines on how to use Double-Take functions and replicas to manually or automatically failover or recover many popular third party applications and a general process to accomplish failover or recovery of many other third party applications. While these steps are believed to be accurate for the specific configuration, Double-Take version, and application versions originally tested, due to the number of possible configurations and variables, NSI Software can only test selected combinations and may provide only limited support for the operation and configuration of third party applications or the behavior of those applications before, during, or after failover, in its discretion. In cases where NSI Software has no direct access to or experience with a particular application or configuration, NSI Software support may also be limited to only the actual replication of the file system data and failover (name and IP address) of the server.

For assistance in validating, implementing or troubleshooting these or other possible configurations with third party applications, NSI Software and its partners may offer professional services on a fee basis to apply best practices for assisting with third party applications to recover automatically or manually using replicated data.

This, and any other, application note is provided solely for the convenience of our customers and is not intended to bind NSI Software to any obligation.

Table of Contents

Introduction	1
Requirements	1
Naming Conventions	2
Protecting Your IIS Data	2
Install Software on the Source	2
Install and Configure Software on the Target	3
Configure and Begin Mirroring and Replication	5
Configure Failover and Begin Failure Monitoring	7
Monitoring Failover	9
Restoring Your IIS Data	11

Introduction

Internet Information Server (IIS) is a standards-based Web and File Transfer Protocol (FTP) server from Microsoft. IIS is designed to operate on the Windows network operating system and is an Internet standards-compliant HTTP (Hypertext Transfer Protocol) server that also includes FTP and several other valuable Web and FTP related services. IIS permits the user to fully design, create, deploy, and manage Web sites of any size.

This document describes the steps necessary to configure Double-Take version 4.x to provide high availability for Windows servers running IIS. These procedures allow a secondary server to assume the identity and role of a failed IIS server while maintaining the availability of IIS services with minimal disruption or data loss.

To complete these instructions, install IIS and Double-Take, and configure Double-Take for replication and failover. Due to the complexities of these applications, this document is intended for network administrators with experience installing, configuring, and maintaining network applications including Double-Take and IIS.

Requirements

- ◆ Two servers that meet one of the following operating system requirements:
 - ◆ IIS 4.0—If you will be using IIS version 4.0, you will need Microsoft Windows NT 4.0 with Service Pack 4 or higher
 - ◆ IIS 5.0—If you will be using IIS version 5.0, you will need Microsoft Windows 2000

NOTE: The two servers should both be running the same operating system.

If you are using Windows NT, it is recommended that both source and target servers be standalone servers. You may experience problems with promotion and demotion during failover if either of the machines are Primary or Backup Domain Controllers.

- ◆ Both servers must be connected to the same physical network
- ◆ One copy of Microsoft Internet Information Server
- ◆ Two licensed copies of Double-Take 4.x
- ◆ The Double-Take Chngname utility

NOTE: The Chngname.exe utility is available on the NSI Software web site at www.nsisoftware.com/updates/chngname.htm.

Naming Conventions

Double-Take provides failover capabilities for multiple source (production) servers to be monitored by and failed over to a single target (high availability) server. When a source server fails, Double-Take causes the target server to add (or optionally replace) the failed server's name and IP address. For most applications, this provides nearly instantaneous failover, with no need to reboot the target server, and it allows server-based applications already running on the target server to continue without interruption. When Double-Take performs failover by adding the failed servers name to the existing name of the target this is known as multi-naming since the target machine is actually broadcasting multiple names on the network and responding for multiple IP address.

Unlike most client-server applications, IIS is sensitive to the primary name of the server on which it is running. If it was installed on server SOURCE, and server TARGET adds the name SOURCE, IIS will not run because the server's primary name is still TARGET. However, with the Double-Take Chngname utility, you are provided the ability to temporarily change the primary name on the target to make failover of name sensitive services, such as IIS, possible.

Protecting Your IIS Data

Install Software on the Source

1. Install IIS on the source, if it is not already installed.
2. Record the drive and directory where you installed IIS. For example, the default directories for IIS are `<drive>:\InetPub\`.

IIS Installation Drive and Directory: _____

3. Install Double-Take 4.x on the source machine using the installation defaults. See the Double-Take *Getting Started* guide for details.

Install and Configure Software on the Target

1. Remove the source machine from the network. This step will allow the target machine to use the source's identity for this section.
2. Change the active server name of the target to the name of the source using the Chngname.exe utility.

NOTE: The Chngname.exe utility is available on the NSI Software web site at www.nsisoftware.com/updates/chngname.htm.

Select **Start, Run** and enter the command:

```
<drive>:\<directory>\chngname /s source_name
```

For `source_name`, enter the name of your source.

3. Now that the target's active server name is identical to the source's name, install IIS on the target using the same drive and directory specifications recorded in step 2 of the previous section.

WARNING: When prompted, *do not* reboot the target machine at this time.

4. In Control Panel, Services, set the IIS services to manual startup. This step allows the Double-Take failover and failback scripts that you will be creating later to control the starting and stopping of the IIS services. (Note which services are specific to the version of IIS that you are using.)
 - ◆ Content Index (IIS version 4.0 only)
 - ◆ FTP Publishing Service
 - ◆ IIS Admin Service
 - ◆ Microsoft NNTP Service (this service may not be applicable to your environment)
 - ◆ Microsoft SMTP Service
 - ◆ World Wide Web Publishing Service
5. Manually configure all web sites which are configured on the source. This includes IP address assignments, virtual directories, security, etc.

NOTE: If any configuration changes are later made to the web sites on the source, the same configuration changes must be manually made on the target.

6. Install Double-Take 4.x on the target machine using the installations defaults. See the Double-Take *Getting Started* guide for details. .

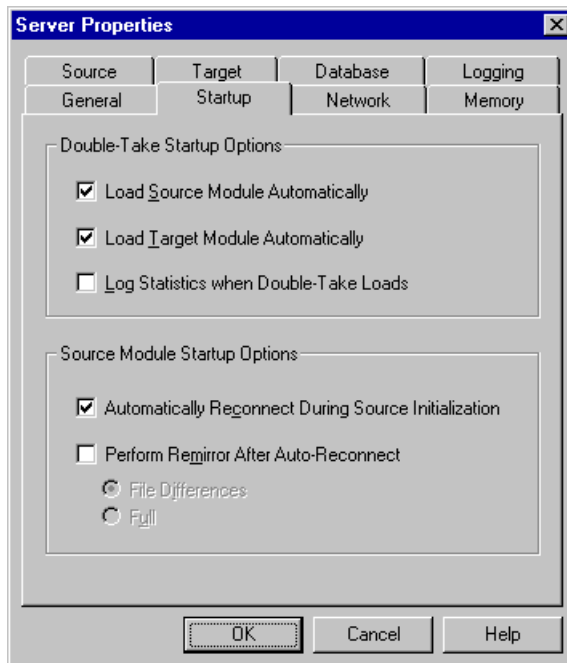
WARNING: When prompted, *do not* reboot the target machine at this time.

7. Modify the Double-Take service so that it interacts with the desktop. Use steps a for Windows 2000 or steps b for Windows NT.
 - a1. Select **Start, Administrative Tools, Services** and double-click the Double-Take service.
 - a2. Select the **Log On** tab and mark the check box **Allow Service to Interact with Desktop**.
 - a3. Click **OK**.
 - b1. In Control Panel, Services, double-click the Double-Take service.
 - b2. Mark the check box **Allow Service to Interact with Desktop**.
 - b3. Click **OK**.
8. Change the active server name of the target back to its original identity by using the Chngname.exe utility. Select **Start, Run** and enter the command:

```
<drive>:\<directory>\chngname /t
```
9. Reconnect your source machine back to the network.
10. Reboot the target machine.

Configure and Begin Mirroring and Replication

1. Select **Start, Programs, Double-Take, Management Console**.
2. Double-click the source machine to log on.
3. Right-click the source machine and select **Properties**.
4. If you are using Double-Take version 4.1 or earlier, you will need to disable auto-remirror on auto-reconnect so that the source does not remirror files after failback. In version 4.2 and later, the source automatically recognizes that a restore is required and will not remirror. If you are using 4.1 or earlier, complete steps a-c below. If you are using 4.2, you can continue with the next numbered step.
 - a. Right-click the source machine and select **Properties**.
 - b. Select the Startup tab.



- c. By default, **Perform Remirror After Auto-Reconnect** will be selected. Disable this option so that the source does not remirror files after failback. Click **OK** to continue.

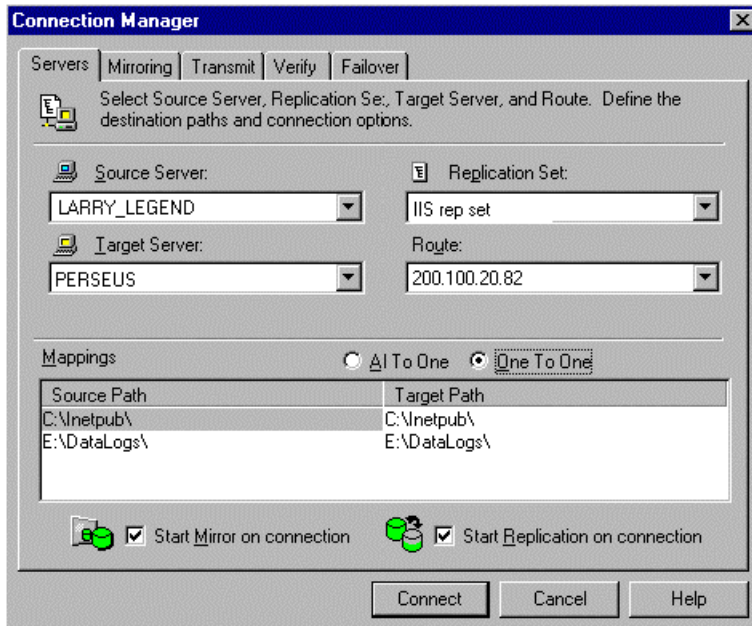
NOTE: If you disable this option and a auto-disconnect occurs, you will need to remirror manually after the connection is reestablished.

5. Right-click your source machine and select **New, Replication Set** and enter the desired name for the replication set.

6. Select the IIS data you want to protect. It is not necessary to replicate the application files since they already exist on the target machine, so you will probably only include the IIS data directories. By default, this is <drive>:\InetPub\. If you have any IIS data stored on other drives, be sure and select those directories as well.

NOTE: The replication set must include all directories that are used by any web sites.

7. Right-click the replication set name and select **Save** to save the replication set.
8. Drag and drop the replication set onto the target. The Connection Manager dialog box opens.



9. The **Source Server**, **Target Server**, **Replication Set**, and **Route** fields will automatically be populated. If you have multiple IP addresses on your Target, verify the **Route** field is set to the correct network path. For detailed information on connecting a source and target, reference the *Double-Take User's Guide*.
10. Select the **One To One** mapping so that the replication set data is transmitted to the same directory structure on the target.
11. Click **Connect** to start the mirror and replication processes.

Configure Failover and Begin Failure Monitoring

1. If a failure occurs, you will want to have the IIS services start on the target machine automatically. To do this, create a batch file called `postover.bat` using the sample batch file below. Save the batch file to the same directory where your Double-Take files are installed.

POSTOVER.BAT

```
rem This command temporarily changes the name of the server. You will need to
rem replace <drive>:\<directory>\ with the location of your Double-Take script
rem files and replace source_name with the name of the source machine. The
rem Chngname utility should be located in the same directory as the
rem Double-Take script files.
<drive>\<directory>\chngname /s source_name

rem If you are using IIS version 4.0, you will need to uncomment the line that
rem starts the Content Index service. Delete the rem characters to uncomment the line
net start "IIS Admin Service"
rem net start "Content Index"
net start "FTP Publishing Service"
net start "Microsoft SMTP Service"
net start "Microsoft NNTP Service"
net start "World Wide Web Publishing Service"

rem This command changes the target name back to its original name. You will
rem need to replace <drive>:\<directory>\ with the location of your
rem Double-Take script files. The Chngname utility should be located in the same
rem directory as the Double-Take script files.
<drive>\<directory>\chngname /t
```

2. After a failure is resolved, you will be ready to bring your source back online. At this time, you will want to stop the IIS services on the target automatically. To do this, create a batch file called `preback.bat` using the sample batch file below. Save the batch file to the same directory where your Double-Take files are installed.

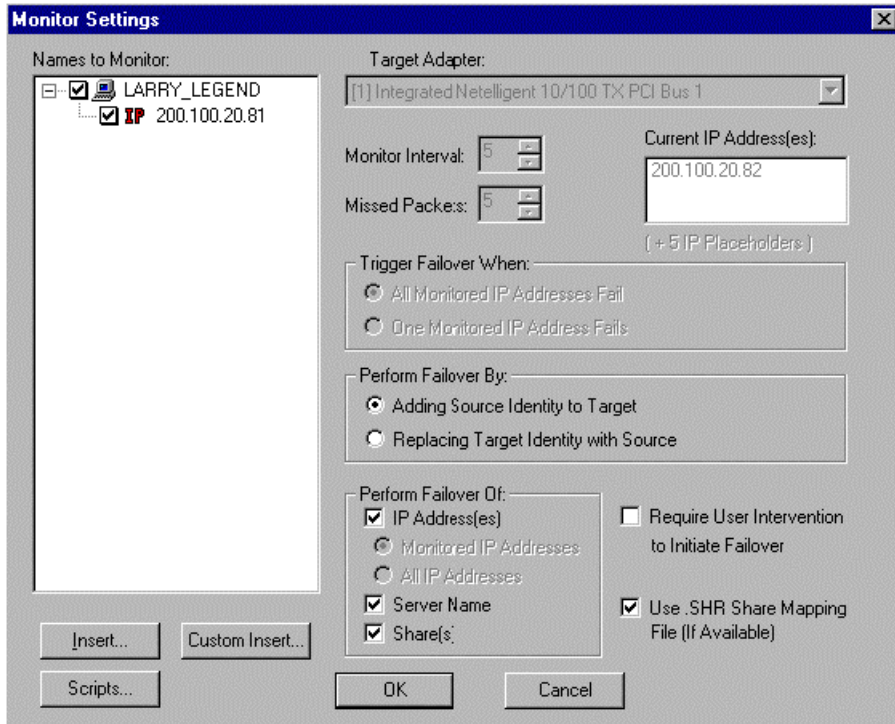
PREBACK.BAT

```
rem If you are using IIS version 4.0, you will need to uncomment the line that
rem stops the Content Index service. Delete the rem characters to uncomment the line
rem net stop "Content Index"
net stop "FTP Publishing Service"
net stop "IIS Admin Service" /y
```

NOTE: These sample batch files are available on the NSI Software web site at www.nsisoftware.com/download/iisscrp.exe.

3. Select **Start, Programs, Double-Take, Failover Control Center**.
4. Select the target machine from the list of available machines. If the target you need is not displayed, click **Add Target**, enter the machine name, and click **OK**.

5. To add a monitor for the selected target, click **Add Monitor**. Type the name of the source machine or click **Browse** to select it, and click **OK**. The Monitor Settings window will open.
6. In the Monitor Settings window, select the IP address that is going to failover and verify that the **Perform Failover By** option **Adding Source Identity to Target** is selected.



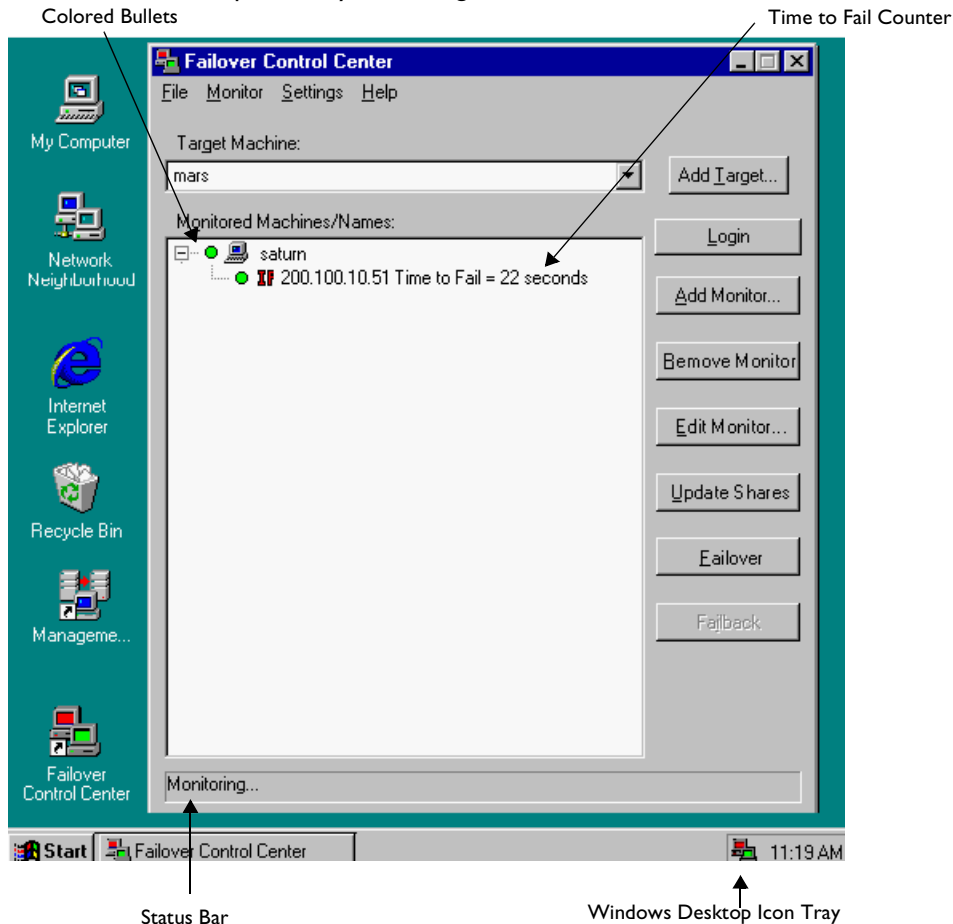
7. Click **Scripts** and insert the scripts that were created in steps 1 and 2 on page 7.
8. Click **OK** to go back to the Monitor Settings dialog box.
9. Click **OK** to begin monitoring the source machine.

In the event of a source machine failure, your target machine is now ready to stand in for your source.

Monitoring Failover

Now that replication and failover monitoring are configured and started, you will need to know if and when there is a problem. Since it can be essential to quickly know the status of your machines, Double-Take offers various methods for monitoring the status of failover. When the Failover Control Center is running, you will see four visual indicators:

- ◆ The Failover Control Center Time to Fail counter
- ◆ The Failover Control Center status bar located at the bottom of the window
- ◆ The Failover Control Center colored bullets to the left of each IP address and source machine
- ◆ The Windows desktop icon tray containing a failover icon



NOTE: You can minimize the Failover Control Center and, although it will not appear in your Windows taskbar, it will still be active and the failover icon will still appear in the desktop icon tray.

The Failover Control Center does not have to be running for failover to occur.

The following table identifies how the visual indicators change as the status of failover changes.

	Time to Fail Countdown	Status Bar	Colored Bullets	Desktop Icon Tray
Source is Online	The Time to Fail counter is counting down and resetting each time a heartbeat is received from the source machine.	The status bar indicates that the target machine is monitoring the source machine.	The bullets are green. ^a	The Windows desktop icon tray contains a failover icon with red and green computers.
Source Fails and Failover is Initiated	The Time to Fail countdown value is 0.	The status bar displays the source machine and IP address currently being assumed by the target.	The bullets are red.	The Windows desktop icon tray contains a failover icon with red and green computers.
Failover is Complete	The Time to Fail counter is replaced with the "Failed Over" message.	The status bar indicates that monitoring has continued.	The bullets are red.	The Windows desktop icon tray contains a failover icon with a red computer.

a. When the **Time to Fail** value has decreased by 25% of the entire timeout period, the bullet changes from green to yellow, indicating that the target has not received a response from the source. The yellow bullet is a caution signal. If a response from the source is received, the countdown resets and the bullets change back to green. If the countdown reaches zero without the target receiving a response from the source, failover begins.

Once failover is complete, any clients accessing the IIS server will be automatically directed to the target.

NOTE: For additional detailed information on failover and other monitoring tools, see the *Double-Take User's Guide*.

Restoring Your IIS Data

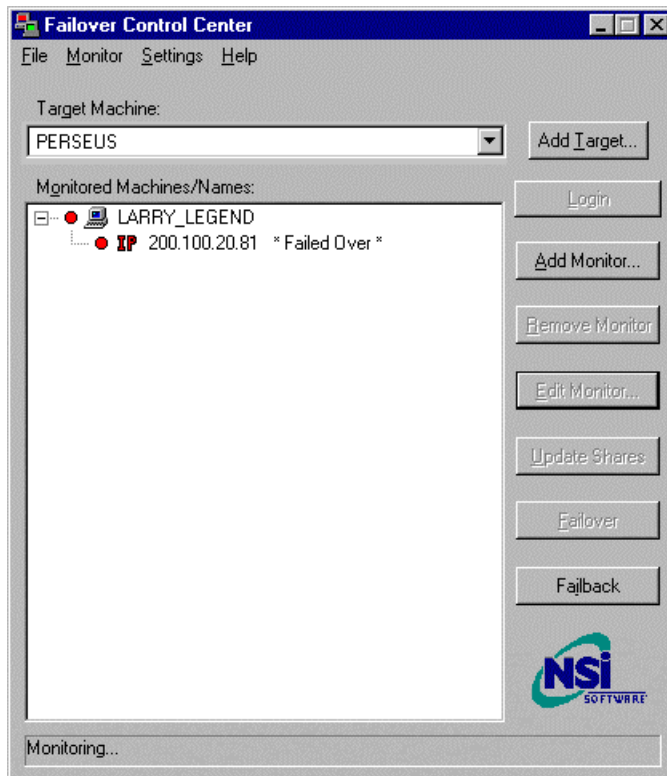
If your source experiences a failure, such as a power, network, or disk failure, your target machine will stand in for the source while you resolve the source machine issues. During the source machine downtime, data is updated on the target machine. When your source machine is ready to come back online, the data is no longer current and must be updated with the new data on the target machine.

1. Make sure the source machine is offline and disconnected from the network.
2. Resolve the source machine problem that caused the failure.

NOTE: If you must rebuild your hard drive, continue with step 3. If you do not need to rebuild your hard drive, continue with step 6.

3. Install Windows and the appropriate service pack, if necessary. Since your source machine is not connected to the network, go ahead and use the source's original name and IP address.
4. Install Double-Take 4.x using the same installation defaults.
5. Install IIS using the same drive and directory settings recorded in step 2 of [Install Software on the Source](#) on page 2.
6. In Control Panel, Services, set the IIS services to manual startup.
 - ◆ Content Index (IIS version 4.0 only)
 - ◆ FTP Publishing Service
 - ◆ IIS Admin Service
 - ◆ Microsoft NNTP Service (this service may not be applicable to your environment)
 - ◆ Microsoft SMTP Service
 - ◆ World Wide Web Publishing Service
7. **Verify that IIS is not running on the source.** The IIS services must not be running at this time. Depending on the type of failure, your services may be set to manual startup, but could still be running. **Stop your IIS services and set them to manual startup.**
8. On the target machine, select **Start, Programs, Double-Take, Failover Control Center**.
9. Select the target machine that is currently standing in for the failed source.

10. Select the failed source and click **Failback**.

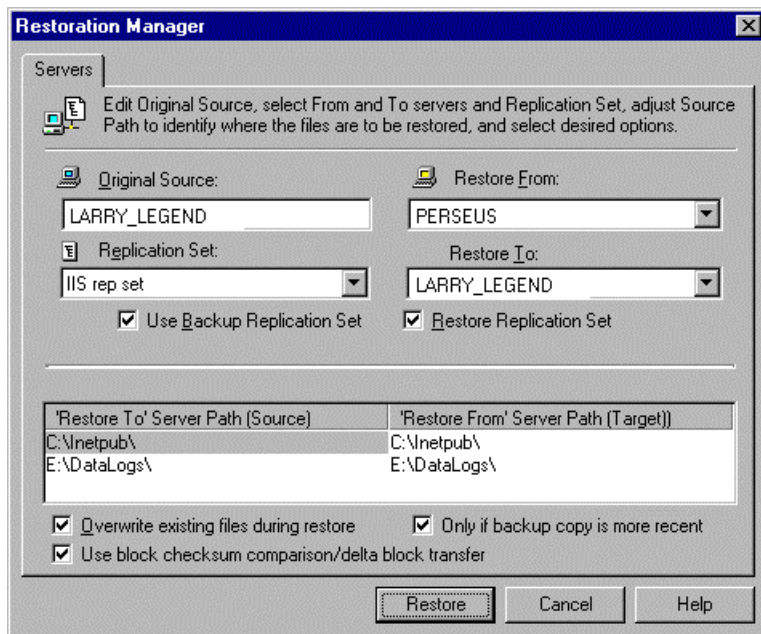


The pre-failback script entered during the failover configuration stops the IIS services on the target so that no additional changes can be made.

11. You will be prompted to determine if you want to continue monitoring the source server. Do not choose **Continue** or **Stop** at this time.
12. Connect the source machine to the network.
13. After the source is back online, select whether you want to continue monitoring the source machine (**Continue** or **Stop**).

14. To begin the restoration process, open the Double-Take Management Console and select **Tools, Restoration Manager**.

NOTE: You can also run the Double-Take DTCL automated restoration script, which can be found in the Double-Take *User's Guide*, to complete the remaining steps in this section.



15. Complete the appropriate fields as described below.
- ◆ **Original Source**—The name of the source machine where the data original resided.
 - ◆ **Restore From**—The name of the target machine that contains the replicated data.
 - ◆ **Replication Set**—The name of the replication set to be restored.
 - ◆ **Restore To**—The name of the machine where you the data will be restored. This may or may not be the same as the original source machine.
16. Identify the correct drive mappings for the data and any other restoration options necessary. For detailed information on the restoration options, see the Double-Take *User's Guide*.
17. Verify that the selections you have made are correct and click **Restore**. The restoration procedure time will vary depending on the amount of data that you have to restore.
18. After the restoration is complete, start the IIS services on the source machine.
19. Reestablish the Double-Take IIS replication set connection.

At this time, your data is restored back to your source machine, the source machine is again the primary IIS server, and, if you selected to continue failover monitoring, the target is available to stand in for the source in the event of a failure.