



HERO BCA User Guide

© 2009,HEROware, Inc. All rights reserved. HEROware, HERO, HERO BCA and HEROguard are Trademarks of HEROware, Inc. Microsoft, Microsoft Windows Small Business Server, Windows and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective companies.

Table of Contents

Table of Contents	3
Introduction 1	5
Full-Server Failover	5
Resources	5
Conventions used in this guide	6
Installation 2	7
System Requirements	7
Installing the HERO BCA Unit	8
Adding the HERO BCA to Your Active Directory Domain	8
Configuring Full Server Failover 3	9
Configuring Full-Server Failover Manager options	10
Saving and reusing configuration options	10
Ensuring a Compatible HERO BCA 4	12
Establishing Server Protection 5	15
Configuring optional settings	17
Monitoring Failover 6	21
Monitoring failover	21
Viewing the log	22
Important Notice – Please Read	23
Starting failover using Full-Server Failover Manager	24
Starting failover from a command line	25
Performing Failback 8	28
Managing Snapshots 9	29
Reverting the Target 10	31
Creating a revertible target image	31
Refreshing the target image	32
Reverting the target	32

Introduction 1

Welcome to HERO BCA User Guide! This manual is for users who want to provide high availability for their entire server. This chapter includes a Full-Server Failover overview, a list of resources available to you while using the HERO BCA, and a list of conventions used throughout this manual.

Full-Server Failover

The HERO BCA Full-Server Failover feature provides high availability for an entire server, including the system state, which is the server's configured operating system and applications. Using Full-Server Failover Manager, you identify your source, which is the server you want to protect, and your HERO BCA, which is the server that will stand-in for the source in the event the source fails. Once the two servers are selected and their configurations validated, Full-Server Failover monitors the source for a failure. When it fails, Full-Server Failover allows the HERO BCA to stand-in for the source by rebooting and applying the source, including its system state, on the HERO BCA. After the reboot, the HERO BCA becomes the source, and the HERO BCA no longer exists. Full-Server Failover is installed with HERO BCA and is activated with your HERO BCA activation code.

Resources

You have many resources available to you when using Full-Server Failover.

Operating System and application documentation—Make sure that you have complete documentation for your operating system and your applications.

HERO BCA documentation—The complete set of HERO BCA documentation includes the manuals listed below. Each manual is available in the C:\Program Files\HEROware\Documentation directory on the HERO BCA and in the root of the installation directory you selected during the installation. The manuals are in Adobe® Acrobat® PDF format. If needed, you can install the free Adobe Acrobat Reader® by downloading the latest version from the Adobe web site at www.adobe.com.

Getting Started Guide—This guide is a complete how-to guide with detailed steps for installing the HERO BCA.

HERO BCA User Guide—This guide is for those users who want high availability for their entire server. It includes instructions for using the Full-Server Failover features. The file name of this manual is User Guide.pdf.

HERO BCA Online Help—The online help can be accessed by pressing the F1 key, clicking the **Help** button on screens where it is available, or selecting **Help, Help Topics**.

Conventions used in this guide

The following conventions are used throughout this guide:

Bold is used for items you click or select with the mouse, such as menu names and items, dialog box options, or button names. For example, when you see **File, Options**, you should select the **File** menu and then choose **Options** from the pull-down menu.

Blue italics is used for cross-references to other sections or chapters in this guide.

`text` is used to indicate text that is displayed on-screen exactly as shown (such as screen messages or error messages) and text that should be entered exactly as shown.

Installation 2

Before installing your HERO BCA, verify that your source server meets the system requirements. Then proceed with *Installing or upgrading Full-Server Failover* on page 2-3.

System Requirements

Each server that will be used as a Full-Server Failover source should meet the following system requirements.

Source Operating System and Licensing

License	Operating Systems
Small Business Server Edition (*)	Windows Small Business Server Edition 2003 or 2003 R2

File System—HERO BCA supports the same file system formats that Microsoft supports: FAT, FAT32, and NTFS.

Disk Usage—The HERO BCA comes with a 1 Terabyte drive capable of accommodating up to that amount of data from the source Small Business Server. If you should require more disk space (you have more the 1 Terabyte of data and applications on your Small Business Server) you should contact HEROware and discuss options for HERO BCA with additional storage capacity.

Protocols and Networking—TCP/IP with static IP addressing or reserved DHCP addressing

Windows Management Instrumentation (WMI)—HERO BCA is dependent on the WMI service. This service must be running in your environment for the HERO BCA solution to work correctly.

Cluster support—HERO BCA does not presently support clustered environments

Installing the HERO BCA Unit

Use these instructions to install your HERO BCA in your environment. It is assumed that at this point you have followed the Quick Start instructions that can be found in the box containing your HERO BCA hardware. Once that is complete, you are ready to follow the installation instructions.

If you have not done so already, follow the instructions detailed in the Getting Started Guide provided in your HERO BCA shipping box to physically install and connect your HERO BCA to your network, monitor, keyboard and mouse.

You are now ready to configure your new HERO BCA.

Adding the HERO BCA to Your Active Directory Domain

This process will add the HERO BCA to your Active Directory (AD) domain to ensure it has access to your Small Business Server for backup and failover purposes.

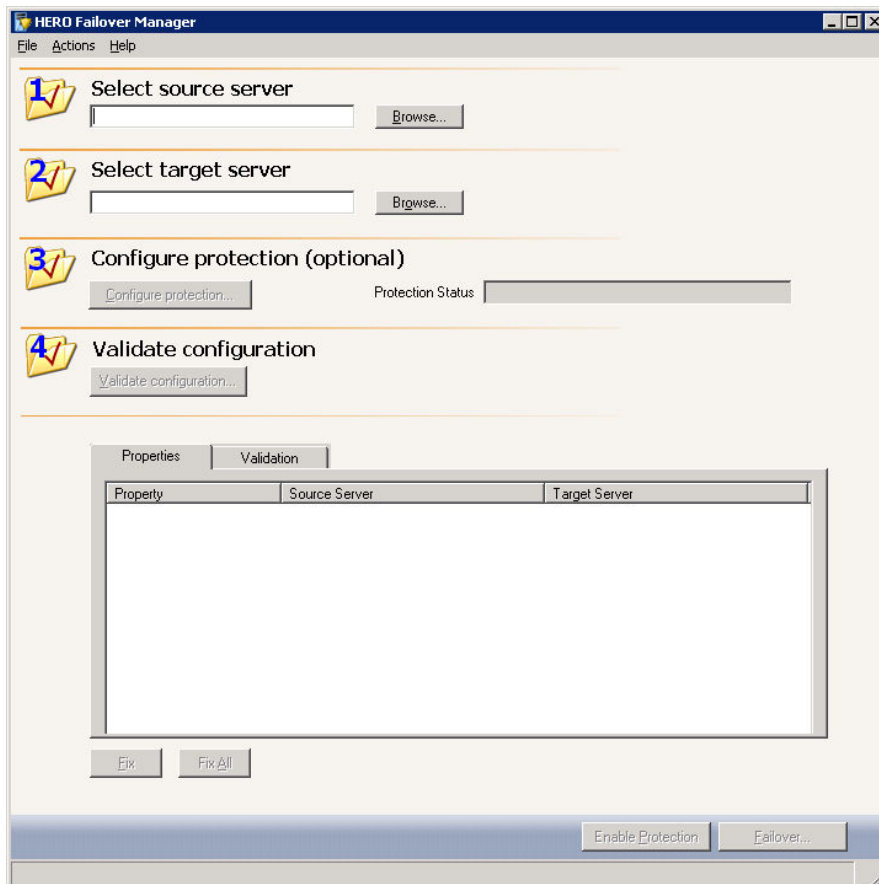
1. On the HERO BCA Windows desktop, double click on the **System** icon.
2. In the **System Properties** dialog window, select the **Computer Name** tab.
3. Click on the Change... button.
4. In the **Computer Name Changes** dialog, you can optionally change the name of the HERO BCA computer by entering a new name in the **Computer Name** field. This is optional.
5. In the Member of section of the **Computer Names Changes** dialog, select the **Domain** radio button.
6. In the **Domain** field, enter the name of your Small Business Server Active Directory Domain.
7. Click the **OK** button.
8. When prompted for credentials, enter the administrator credentials, or other credentials that have administrator rights on the SBS.
9. Click the **OK** button.
10. If the credentials were valid, you will receive a message stating “Welcome to the <Domain Name> domain”. Click **OK** to close this dialog.

You have now added the HERO BCA to your domain and can configure it to provide full failover support.

Configuring Full Server Failover

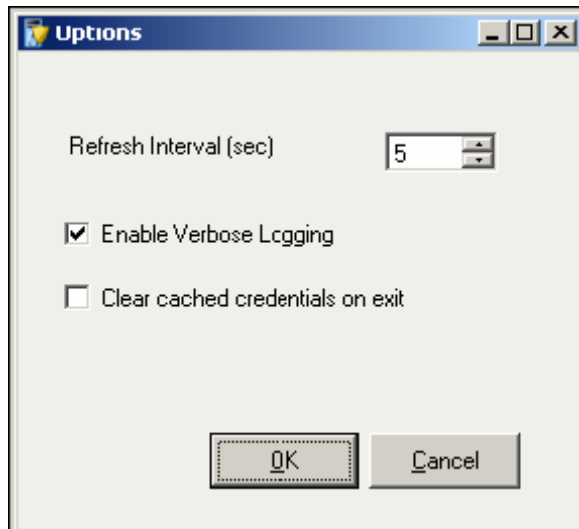
3

Full-Server Failover has its own client called the Full-Server Failover Manager. It allows you to create your source and HERO BCA connection, monitor your high availability protection, manage your Full-Server Failover snapshots, and initiate failover.



Configuring Full-Server Failover Manager options

You can configure options for the Full-Server Failover Manager client by selecting **File, Options**.



Refresh Interval—By default, the main window of Full-Server Failover Manager will automatically update every five (5) seconds. If desired, you can modify the refresh rate. You can also refresh the main window manually by selecting **File, Refresh**.

Enable Verbose Logging—By default, Full-Server Failover Manager creates a log that maintains all processing information. If desired, you can disable the option so that only basic processing information is logged.

Clear cached credentials on exit—By default, Full-Server Failover Manager will save the user credentials supplied for each servers. If desired, you can clear the credentials that are cached so they are not saved. You can also clear the user credentials manually by selecting **File, Clear Cached Credentials**.

Saving and reusing configuration options

After you have created a protection pair and configured any of the optional settings you can save those settings so that you can reuse them for future pairs of servers. Configure your options as defined in *Establishing Server Protection* on page 5-1 and *Configuring optional settings* on page 5-3. Once you have the settings the way you want them, save them by selecting **File, Defaults, Save Current Settings as Defaults**. This creates a file called `FMDefaults.xml`, which will automatically be the default settings the next time you use the Full-Server Failover Manager. If desired, you can rename the `FMDefaults.xml` file and then save a new set of defaults to `FMDefaults.xml` to be used by the Full-Server Failover Manager. This would allow you to have multiple failover configurations, which you can be more easily interchanged. You can also use these different files to initiate failovers without using the Full-Server Failover Manager GUI.

NOTE: Because network adapters are uniquely identified on each server, the **Network Mapping** is not stored in the default settings.

If you want to reset the configuration settings back to the default settings, select **File, Defaults, Reset Defaults**.

Ensuring a Compatible HERO BCA

4

In a high availability protection solution, the HERO BCA you have purchased must be suitable for becoming the source, in the event the source fails. Full-Server Failover will validate the HERO BCA you select and identify any incompatibilities. Errors will disqualify the HERO BCA as a suitable server. To find a compatible HERO BCA, check the table below for each of the requirements.

HERO BCA Configuration

Requirement	Configuration
Operating system version	The source and the HERO BCA must have the same year operating system. For example, you cannot have Windows SBS 2003 on the source and Windows SSE 2008 on the HERO BCA. The two servers do not have to have the same level of service pack or hot fix. (*Note: HERO BCA uses Microsoft Windows Storage Server Editions).
Network adapters	You must map at least one NIC from the source to one NIC on the HERO BCA. If the source has more NICs than the HERO BCA, some of the source NICs will not be mapped to the HERO BCA. Therefore, the IP addresses associated with those NICs will not be available after failover, unless you configure the advanced options. If there are more NICs on the HERO BCA than the source, the additional NICs will still be available after failover.
File system format	The source and the HERO BCA must have the same file system format. For example, an NTFS volume cannot be sent to a FAT volume.
Administrative shares	The Full-Server Failover Manager must be able to access administrative shares on the source and the HERO BCA.

System volume	The HERO BCA must have the same system volume as the source. The system volume is the disk volume that contains the hardware-specific files that are needed to start Windows. The system volume might be the same volume as the boot volume, but that configuration is not required.
Logical volumes	There are no limits to the number of logical volumes, although you are bound by operating system limits. The source and the HERO BCA must have the same number of logical volumes, and the source and the HERO BCA must have the same drive letters. For example, if the source has drives C: and D:, the HERO BCA cannot have drives D: and E:. In this case, the HERO BCA must also have drives C: and D:.
Requirement	Configuration
System path	The source and the HERO BCA must have the same system path. The system path includes the location of the Windows files, Program Files, and Documents and Settings.
HERO BCA path	Full-Server Failover must be installed on the system path on the source.
HERO BCA data state	The source should be from a time when the HERO BCA data state is good. If you are using snapshots, you may want to use a snapshot from the last good data state.
Capacity and free space	<p>The HERO BCA must have enough space to store the data from the source. This amount of disk space will depend on the applications and data files you are protecting. The more data you are protecting, the more disk space you will need.</p> <p>You must also have enough space on the HERO BCA to process and apply the system state data.</p> <p>Full-Server Failover performs several validation checks to determine if adequate disk space is available. First, the HERO BCA must have enough free space on its system volume to hold the entire volume(s) (free and used) from the source. If this first validation check passes, then no additional checks are necessary. Otherwise, there must be at least enough free space on the HERO BCA system volume to store the system path (including the location of the Windows files, Program Files, and Documents and Settings) from the source. If this second validation check passes, then no additional checks are necessary. If this second validation fails, Full-Server Failover will check to see if a previous failover may have been attempted. Since Full-Server Failover can reuse the disk space from a previous failover attempt, it will add the size of that data to the amount of free space available. If that is enough space for the failover, the failover will continue. If not, you will either have to select a different HERO BCA or delete files on the</p>

	HERO BCA to free disk space.
--	------------------------------

Establishing Server Protection

5

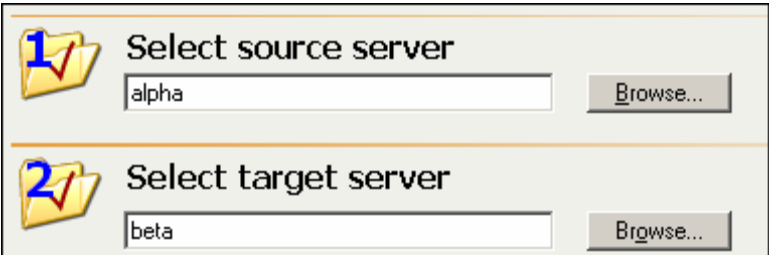
Use the following instructions to establish protection for your source.

1. From the Windows desktop, select **Start, Programs, HERO BCA , Full-Server Failover Manager.**

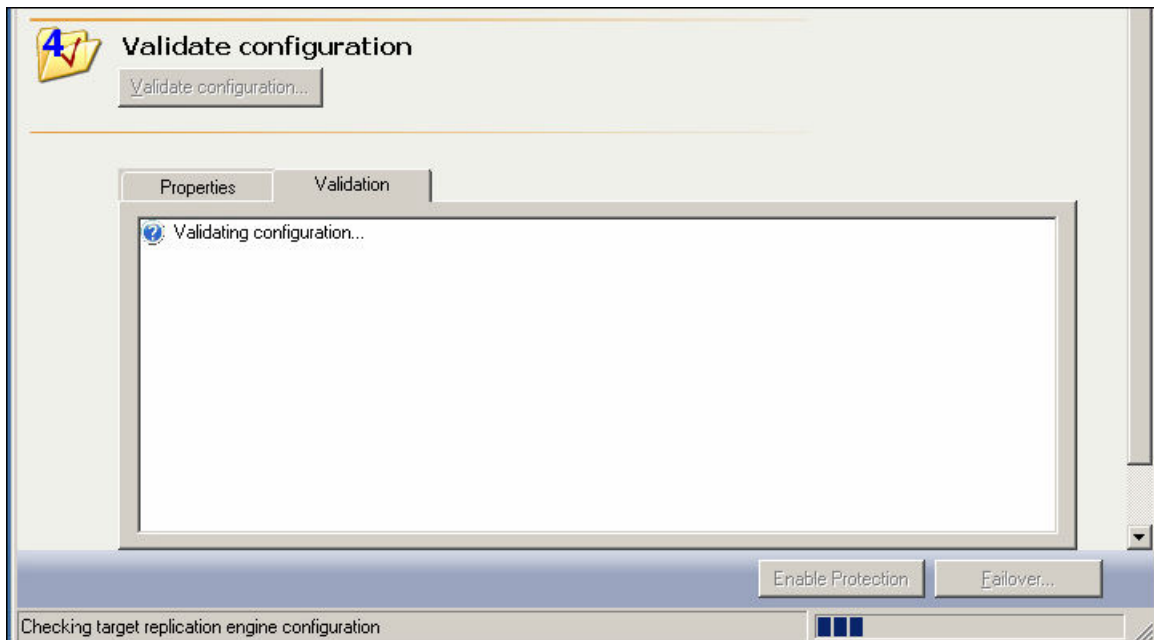
NOTE: The Full-Server Failover Manager cannot be run on Windows 2000 servers because certain actions that are required during the recovery process are not supported by this operating system. You can recover to and from Windows 2000 servers by running the Full-Server Failover Manager on Windows XP or Windows 2003 servers. The user performing any Full-Server Failover tasks must be a member of both the **HERO BCA Admin** and local **Administrators** groups.

2. Enter your source and HERO BCA servers. You can click **Browse** when selecting either server to locate it by drilling down through your network. After you have specified a server name, enter login credentials when prompted. Once the server is selected and logged in, the **Properties** tab at the bottom of Full-Server Failover Manager updates to display the server’s properties.

NOTE: If you select a source that already has Full-Server Failover enabled, the HERO BCA and status of the protection will populate automatically. When logging in, the user name, password, and domain are limited to 100 characters.



3. You can configure optional protection settings, if desired. For details on each of the optional settings, see *Configuring optional settings* on page 5-3.
4. You must validate that your HERO BCA is compatible with your source and can stand-in if the source fails. Click **Validate configuration**. You can also select **Actions, Validate**. The **Validation** tab at the bottom of Full-Server Failover Manager updates to display the validation check. Errors are designated by a white X inside a red circle. Warnings are designated by a black exclamation point (!) inside a yellow triangle. A successful validation is designated by a white checkmark inside a green circle.



Double-click on any of the validation items to see details. You must correct any errors before you can enable protection. Depending on the error, you may be able to click **Fix** or **Fix All** and let Full-Server Failover correct the problem for you. You can also select **Actions, Fix Validation Issues** or **Actions, Fix All Validation Issues**. For those errors that Full-Server Failover cannot correct automatically, you will need to modify the HERO BCA to correct the error, or you can select a different HERO BCA. You must revalidate the selected servers until the validation check passes without errors.

5. Once the validation check passes without errors, click **Enable Protection** to begin monitoring. You can also select **Actions, Enable Protection**.

NOTE: If you have a Full-Server Failover connection established, do not create any HERO BCA connections from the Full-Server Failover source or HERO BCA.

Configuring optional settings

If you want to configure optional protection settings, click **Configure protection** from the main Full-Server Failover Manager window, after you have selected your source and HERO BCA. You can also select **Actions**, **Configure Protection**. There are multiple tabs for different types of protection settings. The **Protection** tab determines what on the source will be protected and how the HERO BCA will handle the protection. The **Failover** tab controls how the failover process will be handled. The **Advanced** tab specifies how the connection between the source and HERO BCA is configured. Review the details below for each of the optional protection settings.

Volumes to include—Select the volumes that you want to protect. You must have the same volumes on the source and HERO BCA. You cannot deselect the boot volume. If you deselect other volumes, you will not be protecting the entire source server.

Directories to exclude—Select the directories that you want to exclude. If you exclude any directories, you will not be protecting the entire source server.

Add—Click **Add** to specify a directory to exclude. Enter the name of the directory or click **Browse** to search for the directory path. Specify **Recursive** if sub-directories of the listed directory should be excluded also. Specify **Non-recursive** if sub-directories of the listed directory should be included. Click **OK** to add the directory to the list of **Directories to exclude**. Repeat this step to add multiple directories.

Edit—Highlight a directory in the list and click **Edit** to modify the directory definition. After modifying the directory, click **OK** to save the changes.

Remove—Highlight a directory in the list and click **Remove** to delete the directory definition. The directory will no longer be excluded.

HERO BCA services—Full-Server Failover Manager determines what services are currently running on the HERO BCA. You can specify which services you want to keep running and those services you want to stop when you enable your protection. Move the services between the **Services to stop** and **Services to leave running** lists by using the double arrows. Select **Show critical services** to see the list of critical services that will remain running on the HERO BCA. The critical services are displayed in a lighter colored, italics font. The critical services cannot be moved from the running list.

Snapshots—A snapshot is an image of data taken at a single point in time. Snapshots allow you to view files and folders as they existed at points of time in the past, so you can, for example, recover from cases where corrupted source data was replicated to the HERO BCA. By default, Full-Server Failover takes periodic snapshots of the data on the HERO BCA. When failover is triggered, you can use the HERO BCA data at the time of failover or you can revert to a snapshot of the HERO BCA data.

Enable periodic snapshots—By default, periodic snapshots are enabled. If you disable snapshots, the data on the HERO BCA at the time of a failure will be used. Because Full-Server Failover uses the Microsoft Volume Shadow Copy service to create snapshots, your HERO BCA must be running Windows 2003 Service Pack 1 or later. If you are using an earlier version of Windows, this option will not be available. Additionally, your source and HERO BCA must be using the NTFS file system. If you are using a FAT file system, the FAT volumes will not be included in the snapshot set, and when the snapshots are reverted, the FAT volume will not be time-consistent with the NTFS volumes.

Snapshot Interval—By default, Full-Server Failover will take a snapshot of the HERO BCA data every 60 minutes. If desired, increase or decrease the interval between snapshots.

Start now—If you want to start taking snapshots immediately after the Full-Server Failover connection is established, select **Start now**.

Start at—If you want to start taking snapshots at a specific date and time, select **Start at** and specify the date and time parameters.

Failover—The **Failover** section configures how failover monitoring occurs.

Manual intervention required—By default, you will be notified when a failover is necessary, but the failover process will not start until you manually initiate it. If you disable intervention, failover will automatically start when a failure is detected.

Monitor Interval—By default, the HERO BCA checks to see if the source is online every five (5) seconds. The source responds back to the HERO BCA when it receives one of these checks. If desired, increase or decrease the interval between checks.

Missed intervals—By default, the HERO BCA can miss five (5) responses from the source before assuming the source has failed. If desired, increase or decrease the number of responses that can be missed before the source is identified as failed.

NOTE: Together, the **Monitor interval** and **Missed intervals** settings determine the total time before failover would be triggered. For example, five missed checks every five seconds would be 25 seconds to trigger failover. To achieve shorter delays before failover, use lower values. To achieve longer delays before failover, choose higher values.

Pre-Failover Script and **Post-Failover Script**—If you want to execute a script on the HERO BCA before failover (**Pre-Failover Script**) begins or after failover has occurred (**Post-Failover Script**), specify the path to the script on the HERO BCA. You can also search for the script by clicking **Browse**. The script will be processed using the same user account that is configured to run the HERO BCA service. Scripts may contain any valid Windows command, executable, batch, or script file. The **Pre-Failover Script** will be executed as soon as the failover process is initiated.

The **Post-Failover Script** will be executed after the failover process ends and the HERO BCA has been rebooted.

Network Mapping—Specify how you want to handle network configurations on the HERO BCA after failover.

Apply source network configuration to the HERO BCA —If you select this option, the source IP addresses will be failed over to the HERO BCA. The IP addresses associated with each NIC on the source will be mapped to the NIC you specify on the HERO BCA. If the source has more NICs than the HERO BCA , some of the source NICs will not be mapped to the HERO BCA , or the HERO BCA NICs may need to be used for more than one source NIC. If there are more NICs on the HERO BCA than the source, the additional NICs will still be available after failover. If you are using a LAN environment, you should select this option.

Retain HERO BCA network configuration—If you select this option, the source IP addresses will not be failed over to the HERO BCA. The HERO BCA will retain all of its original IP addresses. If our HERO BCA is on a different subnet (typical of a WAN environment), you should select this option. The following options are available if you want to update DNS.

DNS Server—The source’s primary DNS server is selected by default. If desired, you can select a different DNS server.

Source Server IP—Select the IP address from the source that you want to remap to an IP address on the HERO BCA.

HERO BCA Server IP—Select an IP address on the HERO BCA that will be replace the source IP address in DNS.

Username—Specify a user that has privileges to access and modify DNS records. The account must be a DNS Admin for the domain in which the DNS server resides. You can enter a user name for a different domain by entering a fully qualified user name. The fully qualified user name must be in the format domain\username or username@domain. If you enter a non-qualified name, the DNS domain will be used by default. The domain name is obtained from the DNS server name, provided that reverse lookup in DNS is enabled.

Password—Enter the password that is associated with the specified user name.

After you have entered the DNS information, click **Test** to validate that DNS is configured correctly and that the specified credentials are sufficient to update DNS. When the DNS configuration is complete, click **OK** to save your entries and return to the Configure Protection window.

Route—By default, Full-Server Failover will select the default route for transmissions. If desired, select a different IP address on the HERO BCA that will be used for Full-Server Failover transmissions.

Mirroring—Select the type of HERO BCA mirroring process you want to perform. A **Full** mirror will transmit all files from the source to the HERO BCA. A **Checksum** mirror will transmit only the blocks of data that are different between the source and HERO BCA.

NOTE: The mirror will remain in an initializing state until the mirror calculation is complete.

Estimate Replication Set size based on volume—If enabled, the replication set size is based on the volume size, which is a faster calculation. If disabled, the replication set size is based on the selected data, which can be a slower calculation.

Compression—Select the level of compression that you want to use. This reduces the amount of bandwidth needed to transmit data from the source to the HERO BCA. The data is compressed before being transmitted and then is uncompressed before it is written on the HERO BCA. If desired, you can also disable **Compression**. Typically, compression is used in WAN environments, but not in LAN environments. After you have configured the settings on the various tabs, click **OK** to return to the main Full-Server Failover Manager window.

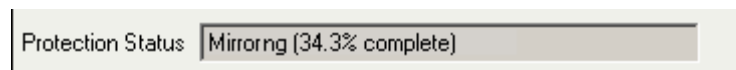
Monitoring Failover

6

After you have enabled protection, you can monitor the protection from Full-Server Failover Manager, and you can review the log file generated by Full-Server Failover Manager.

Monitoring failover

After you have enabled protection, you can monitor the protection from Full-Server Failover Manager. The **Protection Status** is displayed in the right center of Full-Server Failover Manager. You can tell the status of your protection from this field.



Disabled—Protection for the source has not been started. The HERO BCA must be validated as compatible before you can enable protection.

Initializing—Full-Server Failover is initializing protection. Once initialization is complete, mirroring will automatically begin.

Mirroring (% complete)—Full-Server Failover is mirroring the source's data and system state to the HERO BCA. The percentage indicates how much of the mirror has been completed. Protection is not complete until the mirror has completed.

Mirroring (Retrying)—You may see this status message if the HERO BCA is out of disk space or if Full-Server Failover cannot write to a file on the HERO BCA. Check the log file on the HERO BCA for more information.

Mirroring (Mirror stopped)—You may see this status message if your mirroring process has stopped. Depending on the reason for the stopped mirror, it may restart automatically. Check your Full-Server Failover log file. See the *User Guide* for more details on the log file.

Mirroring (Source Unavailable)—You may see this status message if the source has become unavailable during your mirroring process. You cannot failover until the mirroring process is complete. Correct the issues causing the unavailability, and mirroring will restart automatically.

Mirroring (Op Dropped)—You may see this status message if the HERO BCA server cannot apply data to disk. For example, a file may be in use on the HERO BCA. Check the log file on the HERO BCA for more details. See the HERO BCA *User's Guide* for details on the log file.

Enabled—The mirroring is complete and protection of the source is enabled. In the event the source should fail, the HERO BCA will be able to stand-in for it.

Enabled (Source Unavailable)—You may see this message when the HERO BCA has lost communication with the source. If communication is reestablished before the failover monitoring time expires, the status will update to **Enabled**. If communication is not reestablished before the failover monitoring time expires, the status will update to **Failover condition met**.

Failover condition met—The HERO BCA has missed too many responses from the source, indicating that the source has failed. At this time, you need to manually determine the status of the source. If the source is still up and users are accessing it, you need to resolve the communications errors between the source and HERO BCA. Once the communication issue is resolved, the status will update to the appropriate state. If the source is indeed down and users are unable to access it, start failover.

Failing over (% complete)—The HERO BCA is in the process of failing over for the source. The percentage indicates how much of the failover has been completed.

Failed over—Failover is complete. The HERO BCA will automatically reboot. In addition to the status displayed in Full-Server Failover Manager, a log file is generated detailing processing information.

Viewing the log

By default, Full-Server Failover Manager logs basic processing information. To view the log file, select File, Logs, View Full-Server Failover Manager Log. The log file will be opened automatically in Notepad. The log file, `FFMLog.log`, is located on the Full-Server Failover Manager machine in the directory where you installed it. You can clear the log file by selecting File, Logs, Clear Full-Server Failover Manager Log.

Initiating Failover

7

In the event your source has failed, you can failover to your HERO BCA allowing for immediate availability. Failover can be initiated through the Full-Server Failover Manager client. You also have the option of initiating failover by using a command line interface.

Important Notice – Please Read

When initiating a failover it is very important to understand the consequences and new environment that is created. When a failover is initiated, the following situations will occur:

- The HERO BCA that you will failover to will be formatted to replace your failed Microsoft Small Business Server (SBS) and will provide you with a fully functional, identical SBS available for production use.
- Once the failover is complete, there will be no backup or failover available for the HERO BCA that is running your SBS until you implement such a failover or backup.
- During this period of no backup, your SBS server is at risk. That is to say that your SBS is dependent on a single point of failure (the hard drive in the HERO BCA).

You **MUST** implement a new failover or backup strategy as soon as possible. To do this, you may use the HEROguard online service; purchase a new HERO BCA or failback to the original SBS physical server once the cause of failure has been resolved.

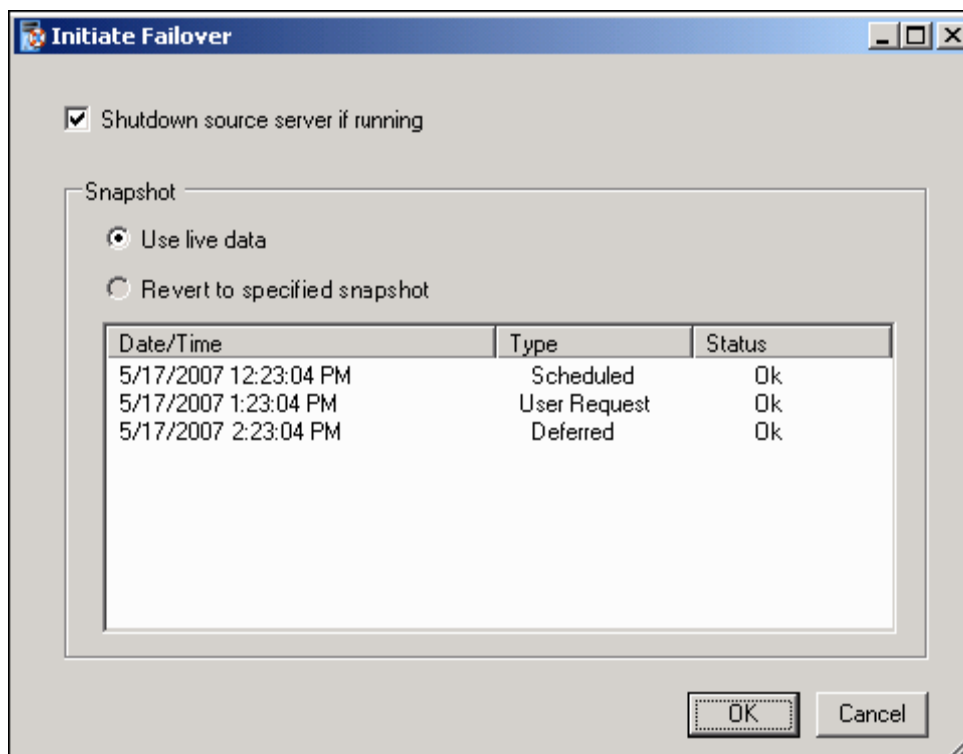
Once a failover occurs and the HERO BCA has taken on the identity and services of your original SBS, the HERO BCA has worked as documented. It is the client's responsibility to ensure a new failover or backup strategy is implemented as soon as possible. HEROware Inc. is not responsible for any loss of data or availability due to any failure, hardware or software, on the HERO BCA.

Starting failover using Full-Server Failover Manager

When a failover condition is met, you will want to start failover. Additionally, you can start it without a failover condition, as long as protection is enabled. For example, you may want to force failover when upgrading to a better source server.

To start failover, click **Failover**. You can also select **Actions, Failover**.

If Full-Server Failover determines there is a possibility that the data on the HERO BCA is incomplete, you will be warned before failover begins. If you proceed with failover, the state of the source will be unknown until failover is complete. The best case scenario would be a missing data file, while the worst case scenario would be missing system state data that causes the server to be unusable or unbootable.



Shutdown source server if running—If the source is still running, Full-Server Failover Manager can stop it. Although, if Full-Server Failover Manager cannot communicate with the source, the shutdown command will fail. This option prevents network conflicts in those cases where the source and HERO BCA are still both running and communicating, such as a forced failover.

Use live data—Select this option to use the data on the HERO BCA at the time of failover.

Revert to specified snapshot—Select this option, and then select a snapshot. The data on the HERO BCA will be reverted to the selected snapshot. This option will not be available if there are no snapshots on the HERO BCA or if the HERO BCA does not support snapshots. To help you understand what snapshots are available, use the **Type** and **Status** columns. The **Status** indicates the state of the connection

between the source and HERO BCA at the time the snapshot was taken. The **Type** information is displayed in the following table.

Type	Description
Scheduled	This snapshot was taken as part of a periodic snapshot.
Deferred	This snapshot was taken as part of a periodic snapshot, although it did not occur at the specified interval because the connection between the source and HERO BCA was not in a good state.
User Request	User Request This snapshot was taken manually by a user.

Click **OK** to initiate failover. Monitor the failover percentage as shown in the **Protection Status**. At the end of failover, the HERO BCA will be rebooted automatically. After the reboot, the HERO BCA will no longer exist, since it will become the source.

NOTE: Because the Windows product activation is dependent on hardware, you may need to reactivate your Windows registration after failover. Follow the on-screen prompts to complete the reactivation.

If you are failing over a cluster node, it is possible that volumes may lose their drive letter assignments. If a clustered application fails to start after failover and the disk signature has changed, check the drive letter assignments under the Disk Management utility and re-create drive letter assignments as needed.

Starting failover from a command line

You can configure connections and initiate failover without using the Full-Server Failover Manager user interface. The same executable that launches the user interface can be used from a command prompt with options. The command line execution opens the user interface, passes through specified parameters, and initiates specified processes. You may want to use this alternate execution if you have different configuration files that you want to execute or if you have multiple connections. The Full-Server Failover Manager command can be initiated one at a time from a command prompt, or it can be scripted.

The Full-Server Failover Manager executable is located in the installation directory.

Command	FFManager
Syntax	FFMANAGER /SOURCE <i>source_name</i> /HERO BCA <i>HERO BCA_name</i> /USERNAME <i>username</i> /PASSWORD <i>password</i> /VALIDATE /FIXALL /PROTECT /FAILOVER /LOGLEVEL <i>number</i> /CONFIG <i>filename</i>

<p>Options</p>	<p>SOURCE <i>source_name</i>—Name of the source</p> <p>HERO BCA <i>HERO BCA_name</i>—Name of the HERO BCA</p> <p>USERNAME <i>username</i>—Name of a user who is a member of the HERO BCA Admin security group</p> <p>PASSWORD <i>password</i>—Password associated with the specified user</p> <p>VALIDATE—Validates the configuration of the two servers to make sure they are compatible</p> <p>FIXALL—Corrects those errors that Full-Server Failover can automatically correct</p> <p>PROTECT—Initiates the connection between the source and HERO BCA</p> <p>FAILOVER—Initiates failover from the source to the HERO BCA</p> <p>LOGLEVEL <i>number</i>—Specifies the level of detailed logged based on the following numbers.</p> <p>2—Informational messages are logged</p> <p>3—Informational and error messages are logged</p> <p>4—Informational, error, and exception messages are logged</p> <p>5—Informational, error, exception, and debug messages are logged. This is the default setting.</p> <p>6—Informational, error, exception, debug, and internal coding messages are logged</p> <p>CONFIG <i>filename</i>—Name of the file that contains the failover options. If no file is specified, the FFMDDefaults.xml file will be used.</p>
<p>Examples</p>	<pre>ffmanager /source alpha /HERO BCA beta /username administrator /password password /validate /fixall /protect</pre> <pre>ffmanager /source alpha /HERO BCA beta /username administrator /password password /validate /failover</pre>

Notes	If you do not specify any options with this command, the Full-Server Failover Manager user interface will open. The fields will be blank and no processing will occur.
--------------	--

Performing Failback

8

After your HERO BCA has failed over and becomes your source, you can stay with that configuration long term. However, in some instances, it may be necessary or desired to go back to using the original hardware after you have failed over. Use the following process to failback to your original (or other) hardware.

1. Because your new source is on the network, you must make sure your original source is unique on the network to avoid name and IP address conflicts. You have several options available for achieving this.

Reinstall Windows using unique server information. This may be the best option if your original source was a domain controller or running a name-specific application like Exchange.

Run a utility like Microsoft SysPrep to modify SIDs (security identifiers), IP addresses, and the server name.

Manually make the original source unique by modifying IP addresses and the server name. If your original source was a domain controller, you must also modify the SIDs.

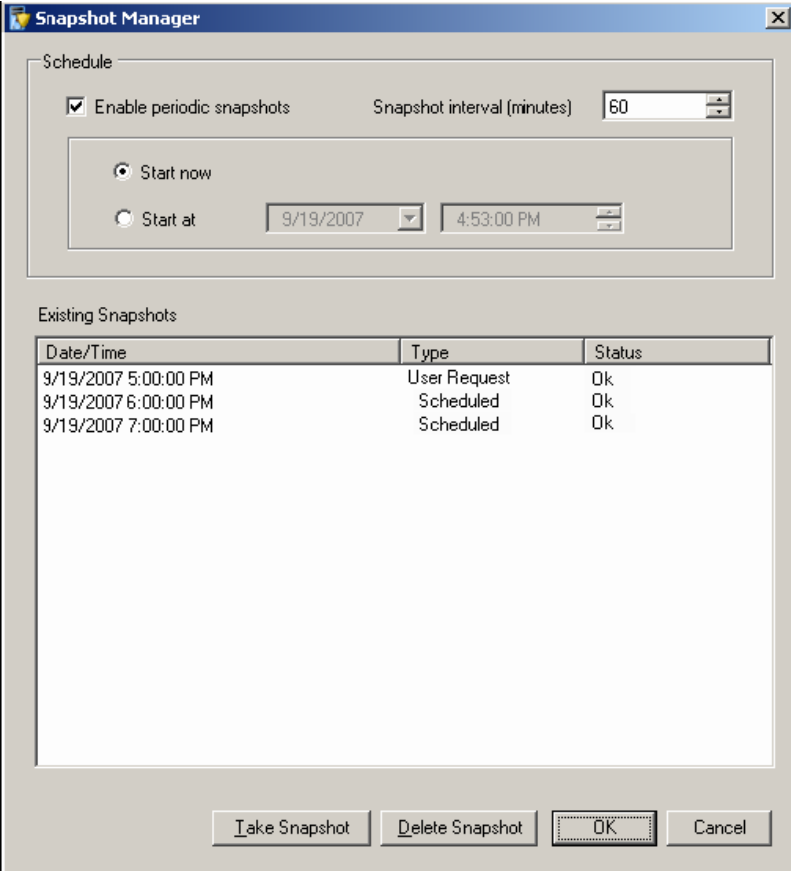
2. Establish protection from your new source to your original source using the same process as when you protected your original source. See *Establishing Server Protection* for details.
3. When the protection has been established from your new source to your original source, initiate failover. See *Initiating Failover* for details.

Once failover has completed, you will be back to your original hardware.

Managing Snapshots

9

By default, snapshots are enabled in Full-Server Failover. Also by default, a snapshot is taken every 60 minutes. This may lead to numerous snapshots on the HERO BCA that you may want to manage. You can do that by selecting **Actions, Snapshot Manager**. (This option is only available when a source and HERO BCA are selected and protection is enabled.)



Enable periodic snapshots—By default, periodic snapshots are enabled. Because Full-Server

Failover uses the Microsoft Volume Shadow Copy service to create snapshots, your HERO BCA must be running Windows 2003 Service Pack 1 or later. Your source and HERO BCA must also be using the NTFS file system. If you are using an earlier version of Windows or a FAT file system, this option will not be available. If you disable snapshots, the data on the HERO BCA at the time of a failure will be used.

Snapshot Interval—By default, Full-Server Failover will take a snapshot of the HERO BCA data every 60 minutes. If desired, increase or decrease the interval between snapshots.

Start now—If you want to start taking snapshots immediately after the Full-Server Failover connection is established, select **Start now**.

Start at—If you want to start taking snapshots at a specific date and time, select **Start at** and specify the date and time parameters.

Take Snapshot—If you want to take a snapshot manually (outside of the specified interval), click **Take Snapshot**.

Delete Snapshot—If you no longer want to keep a snapshot, you can delete it by highlighting the snapshot in the **Existing Snapshots** list and clicking **Delete Snapshot**. To help you understand the snapshots, use the **Type** and **Status** columns. The **Status** indicates the state of the connection between the source and HERO BCA at the time the snapshot was taken. the

Type	Description
Scheduled	This snapshot was taken as part of a periodic snapshot.
Deferred	This snapshot was taken as part of a periodic snapshot, although it did not occur at the specified interval because the connection between the source and HERO BCA was not in a good state.
User Request	User Request This snapshot was taken manually by a user.

NOTE: The **Schedule** options at the top of the Snapshot Manager are the same options from the Configure Protection **Protection** tab. If you change the options in one location, they will be changed in the other location too.

The **Existing Snapshots** list only contains snapshots from Full-Server Failover.

Snapshots from other utilities and tools will not be listed.

Reverting the Target (HERO BCA)

10

When failover occurs, the target (HERO BCA) stands-in for the source by rebooting and applying the source, including its system state, on the target. After the target reboots, the target becomes the source, and the target no longer exists. If you decide to failback to your original hardware, you can revert your HERO BCA back to its original state.

Creating a revertible target image

In order to revert your target, you must have an image of your target to revert to. By default, this revertible image was configured to be created automatically when you established your source protection. If you disabled the creation of this image (by deselecting **Revert Image Volume** on the **Advanced** tab of the optional protection settings), no image of the target was created when protection was established. However, you can create an image of the target after protection has already been established.

1. From the Full-Server Failover Manager, specify your source server and provide credentials, if prompted. The target will automatically populate.
2. Open the Revert Manager by selecting **Actions, Revert Manager**.
3. Select the **Configuration** tab.
4. Select **Enable Target Revert** and specify the volume on the target where you want to store the image of the target. The amount of free space on the selected volume will be displayed along with the location on that volume where the target image will be stored.
5. Click **Apply**. The selected volume will be validated. If there is enough space to store the image of the target, mirroring will begin. If there is not enough space, you will have to select another volume.

You can monitor the **Status** of the target image from the Revert Manager.

Refreshing the target image

1. From the Full-Server Failover Manager, specify your source server and provide credentials, if prompted. The target will automatically populate.
2. Open the Revert Manager by selecting **Actions, Revert Manager**.
3. From the **Revert** tab of the Revert Manager, you can see the date and time when the target image was last updated. If desired, you can update the image of the target by clicking **Refresh Image**. You can monitor the **Status** of the target image refresh from the Revert Manager.

Reverting the target

Use the following instructions to revert your target after failback. Remember, if you are reverting your target and have not performed failback, you should proceed with caution. Without failback, if you revert your target, your source will no longer exist, meaning all of your source data will be lost. Only revert your target if you have failed back or your source data is completely available on another machine.

1. From the Full-Server Failover Manager, specify your original source for the source server and provide credentials, if prompted. The target will automatically populate.
2. Open the Revert Manager by selecting **Actions, Revert Manager**.
3. On the **Revert** tab, **click Revert**.

You can monitor the **Status** from the Revert Manager or from the main Full-Server Failover Manager console. When the revert process is complete, the target will automatically reboot. After the reboot, the target will be back to its original identity and state of the target image.