



# Defender

## Basic Installation and Setup Guide

---

Version 4.2.0

# Contents

## Start

<b>Overview</b>	<b>3</b>
<b>Prerequisites</b>	<b>4</b>
<b>Terminology</b>	<b>5</b>
<b>Defender Plus Requirements</b>	<b>6</b>

## Setup

<b>Double-Take® – Installation &amp; Configuration</b>	<b>7</b>
<b>Production Server(s)</b>	<b>7</b>
<b>Adding a Server to the Console</b>	<b>7</b>
<b>Push Client Installation</b>	<b>10</b>
<b>Manual Client Installation</b>	<b>13</b>
<b>Configure a Replication Job</b>	<b>18</b>

## Server Failback

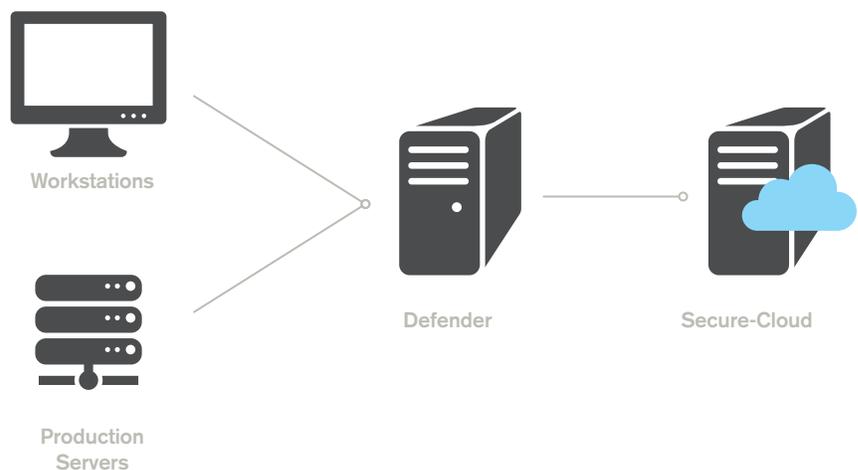
<b>Double-Take® – Prepare &amp; Execute a Failback</b>	<b>27</b>
<b>Configure a Files and Folder Job</b>	<b>27</b>

## Overview

The HERO-Defender (aka Defender) is a self-contained high availability, backup, disaster recovery and business continuity appliance. Utilizing Microsoft® Hyper-V technology the Defender can replicate production MS 2003 and newer servers in real time. This is done by initially mirroring the production server to a virtual machine and then maintaining current updates through continuous real time replication. In the event of a failed server the Defender will spin up the replicated VM within a few minutes.

The Defender also serves as a traditional on premise backup solution storing critical data for both servers and workstations. With the flexibility to retain multiple versions of backups, files and data can be retrieved from any defined point in time. Coupled with HEROware's Secure-Cloud solution, off-site backups have never been easier. The Defender sends backups to HEROware's Secure-Cloud maintaining a bootable version of your protected server(s) in case of a total disaster.

The HEROware Defender & HEROware Secure-Suite platform is a one, two punch for total data protection and recovery.



## Prerequisite

Protecting your production servers requires a few critical steps before the Defender can fully protect them. Please make sure the following patches and or tasks have been completed before moving forward.

- NET 3.5 – All protected servers must have the .NET framework installed. (<http://www.microsoft.com/en-us/download/details.aspx?id=21>) This may or may not require a reboot after installation, however, it is highly recommended that you reboot the server.
  - C++ update – upon installation of the replication client (Double-Take), the software will check for this update and apply it if not present. This step does not require a reboot.
  - For optimum performance in the replication process it is recommended that the source (Server) have a least 5GB of available disk space and 4GB of RAM. Low system resources may cause performance issues when replicating especially when using MS2003 server(s).
  - It is not recommended to run other backup software that may cause file or folder locks during the replication process.
  - Protected server(s) should have a static IP assigned and so should the Defender.
  - It is recommended that that Defender be joined to the Domain. If not joined to the domain host records should be added to the host table to ensure name resolution.
  - Defender is designed to run on the same subnet as the source server(s). DNS resolution is critical especially using crossing subnets.
  - It is recommended that ports 7070 and 7071 on your firewall are opened to the Defender for automated licensing assignment. Additionally ping should be enabled on both source and target.
-

# Terminology

Throughout the user's guide you will hear specific terms used to identify components and or processes. Below is a definition of these terms.

**Source** – Source is the device that needs protection. Usually a Server or Workstation is referred to as the source. Just think source is where the data originates.

**Target** – Target is where the data is protected or replicated. In most cases the target is your Defender or HEROware Secure-Cloud service.

**Secure-Client** – The client configures the job(s) and is installed on the production server(s) and or workstation(s).

**Secure-Server** – The server is installed on your Defender and listens for clients. Used to monitor all jobs and recommended avenue for reporting and alerts.

**Secure-Suite** – HEROware Secure-Suite encompasses both Client & Server products coupled with all associate plug-ins.

**Plug-Ins** – Reference to various modules within the Secure-Suite that allow you to perform specialized backups for Exchange, SQL, ADI (Advanced Disk Image), Hyper-V, etc.

**Replication** – Is the technology used to enable the job created in Double-Take to move data in real time from the Source to the Target VM in Microsoft© Hyper-V.

**VM** – Stands for “Virtual Machine” and holds all the parameters that create the environment that enables the physical server to be virtualized on the Defender using Hyper-V.

**VHD** – The “Virtual Hard Disk” is the replica of the source servers hard disk stored on the Defender.

**Hyper-V** – Name for Microsoft's “Hyper Visor” that enables VM's to be created or hosted on the Defender.

**Host** – References the Defender or HEROware Cloud. Also can be the target.

---

## Defender Plus(+) Requirements/Recommendations

If you purchase the Defender+ package then you will be using your own hardware to create a Defender. A few things to consider when selecting appropriate hardware for your Defender+ Appliance:

- Use Quad-core Intel® or Xeon® processor for best results.
- The processor must support multi-threading to allow virtual machines to be created.
- Reserve at least 4GB of memory for the OS and 4GB for each additional VM, (Recommend 8GB minimum for base 1:1 Defender).
- Recommend building a dedicated OS volume assigned to its own drive and a separate Data volume on one or multiple drives for best performance.
- Size your Data volume based on the storage used on your source server(s) and how much data is to be protected. Also include any other backup plans you have for sizing Defender storage. As a general guideline, we recommend allocating 3x the space from the protected servers.
- Also consider utilizing some form of RAID to protect against Hard Disk failures.
- When preparing to initiate backups to Secure-Cloud, contact HEROware sales or support team to determine the need for a seed drive.
- Utilize a Gigabit NIC for best results.

If your hardware has met the requirements above continue to follow the Prerequisites list and ensure Defender+ is installed correctly.

---

# Double-Take® Installation and Configuration

Your Defender comes preinstalled with Microsoft® Standard 2008 R2 Server running Hyper-V, Double-Take® High Availability; HEROware Secure-Suite, and a Kaseya Agent providing access to HEROware RMM and our Defender Module. No additional software installation is required on the Defender.

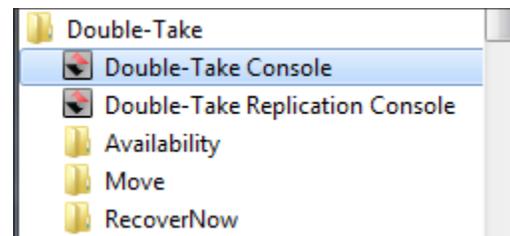
## PRODUCTION SERVER(S)

Preparing your production server for replication is simple. Note: Prerequisites sections should have been completed to ensure a smooth installation. (All software installations should be planned in a maintenance window in case a reboot is required.) HEROware recommends that you patch your servers to aid the installing process.

There are two ways of installing the Double-Take® client on your production servers: Push & Manual.

## ADDING A SERVER TO THE CONSOLE (Clients must be loaded first)

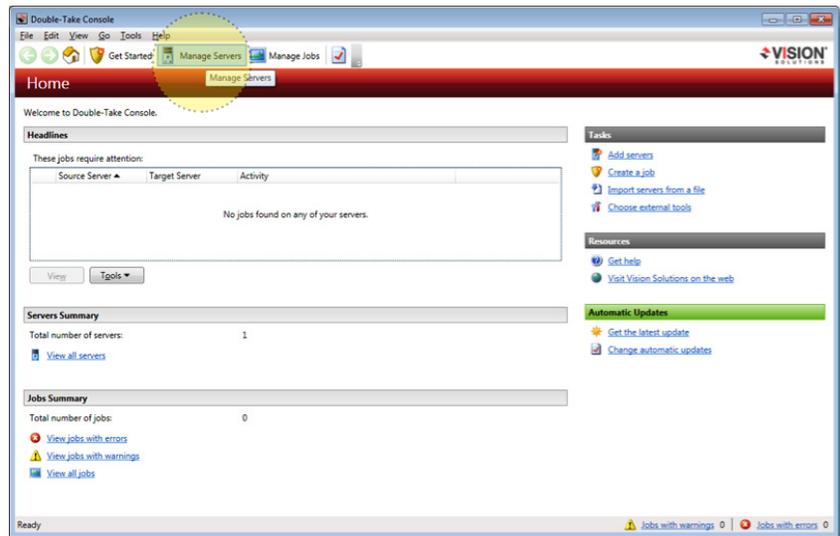
Before you can install Double-Take® software to your source servers you must add them to the DT Console. On the Defender run the Double-Take® Console icon under All Programs and Double-Take.



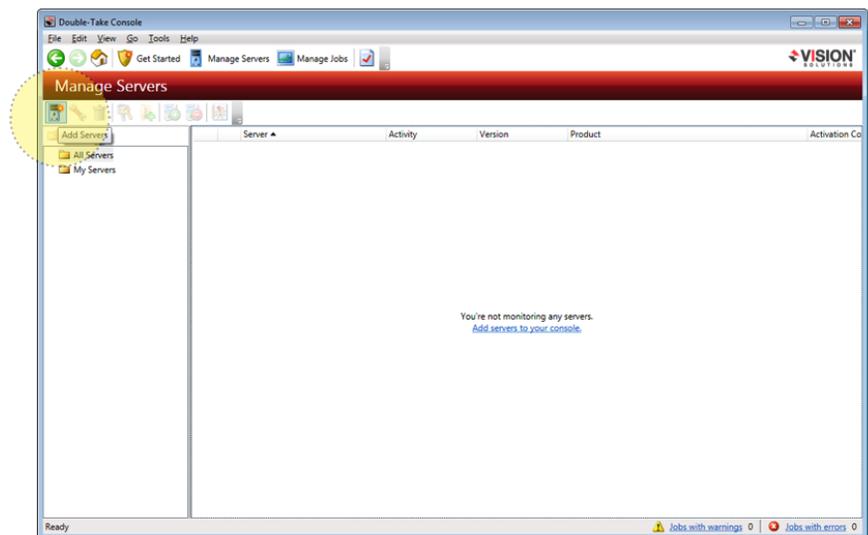
Be patient - this program may take a minute to load. While you're waiting take note of all the IP address of the server(s) you are going to protect including the Defender, these should all be static IP's.

### Adding a server to the console continued...

Once you have the Double-Take® Console displayed we need to add the servers using the Manage Servers icon,

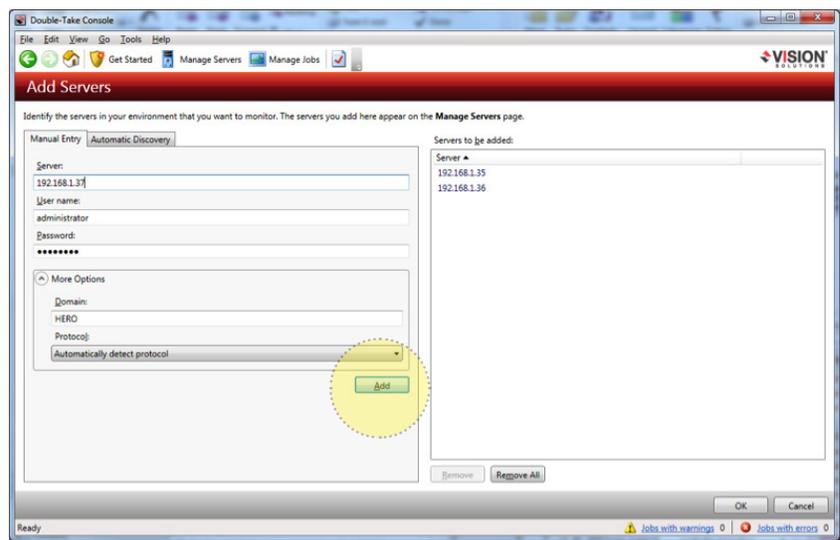


Add the server(s) using the Add Server button as indicated,



### Adding a server to the console continued...

Enter the IP address and credentials for each server including the Defender. If you expand the domain field is available. Once added the server(s) will show up in the right pane labeled "Servers to be added:".



*Note: It is strongly recommended that you create a backup domain user with admin rights and use these credentials when adding your production server(s). The reason is this password should not be changed to ensure connectivity between the source and target. Also when adding the Defender please use the local Administrator account as this is the account used when building your Defender and will have all the proper rights. (If you decide to use the domain user you created for the Defender please add this user to the local Administrator's group and the Double-Take® Admin's group.)*

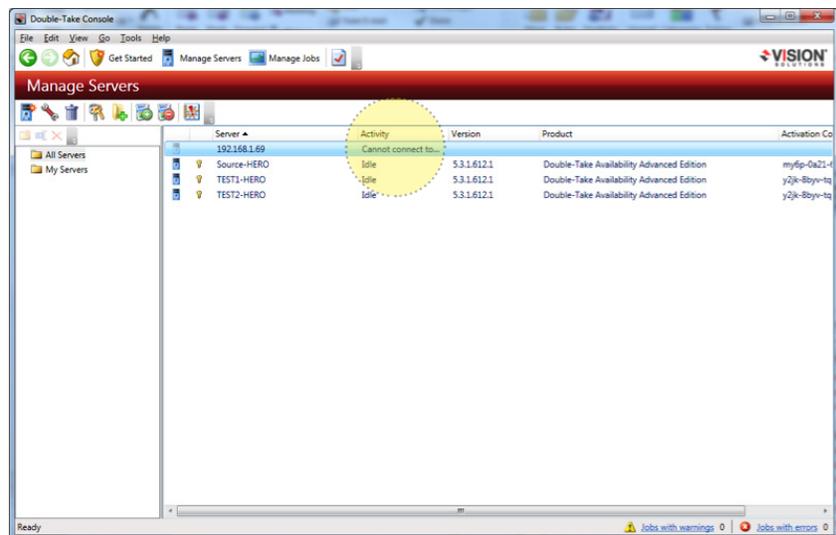
After you have added all the server(s) to be protected, select OK.

## Push Client - Installation

The Manage Servers screen displays all of the servers you added and if DNS is working properly it should resolve the name(s) of all running Double-Take® installations.

In a new installation, Double-Take® is not installed and the IP address is not resolved. Also the Activity column will indicate “Cannot connect to...” This normally means that Double-Take® is not available and needs to be installed. In the example below we added a fourth server to show you the symptoms.

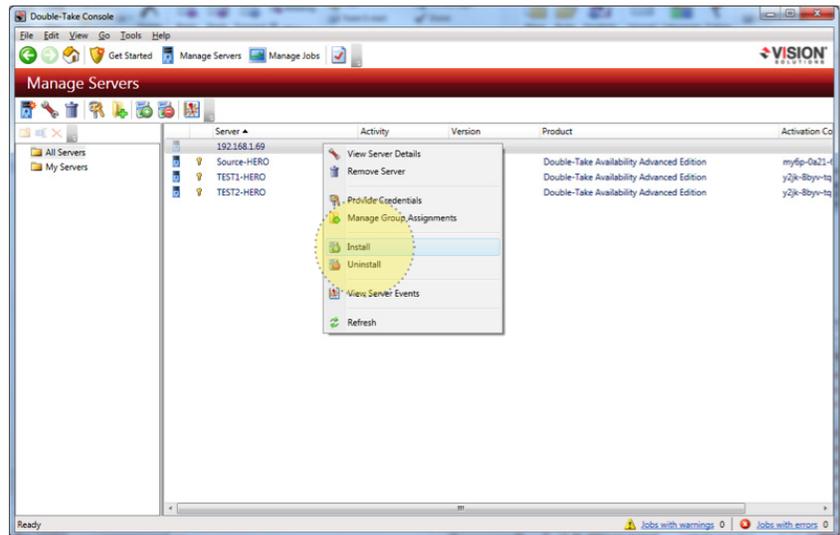
Before you begin to push the service out you should have Double-Take® **Activation Codes** that were emailed to you previously. If you do not have your activation codes then you should contact HEROware sales or support team before going any further



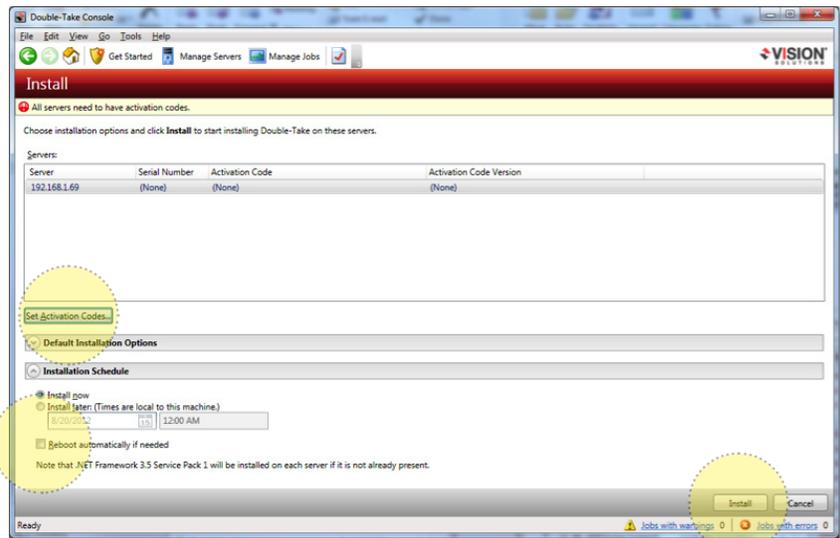
*Note: you are assigned one activation code for each protected server. These codes are assigned by sales and should not be duplicated or your replication jobs will fail to start.*

### Push Client Installation continued...

Select the IP or server you wish to install Double-Take® by simply right clicking and selecting Install.

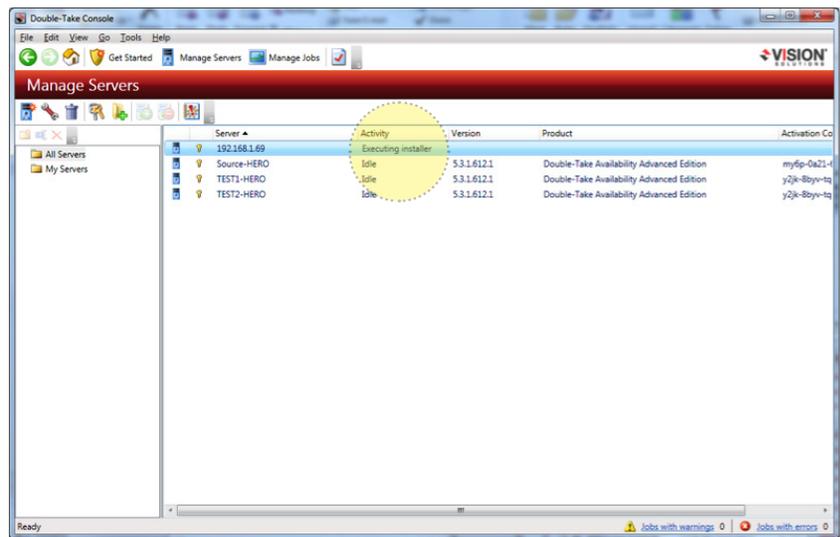


Select the Set Activation Codes... button and add your code. **It's important to uncheck "Reboot automatically if needed"**. If you ran through the prerequisites check list in the beginning no reboot is needed. Click Install when finished.

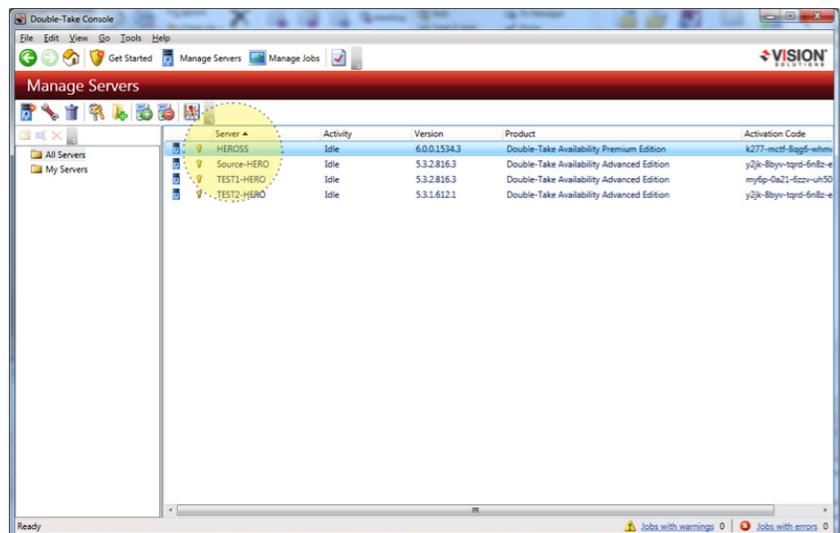


### Push Client Installation continued...

You'll notice under the Activity column the server shows "Executing Installer", this process can take up to several minutes.



Once complete, notice the server column resolved the IP address to the server name meaning that the DNS is working. Double-Take® relies heavily on DNS resolution and it's important that the sources and target can resolve each other forward and backward.



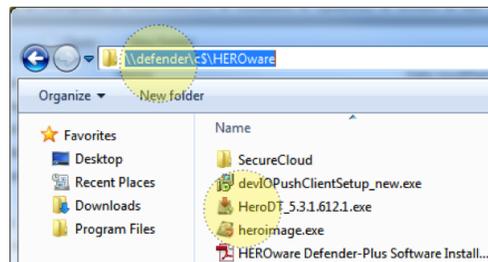
## Manual Client - Installation

Every Defender has a HEROWare folder located on the root of the C: drive. This folder includes the installation program to install Double-Take® manually. As mentioned in the Push Installation instructions, Double-Take relies on DNS and if the source or target cannot resolve each other or you did not complete the prerequisites section by installing .NET 3.5 framework, you may need to install the software manually. Either way it is still highly recommended you complete the prerequisites.

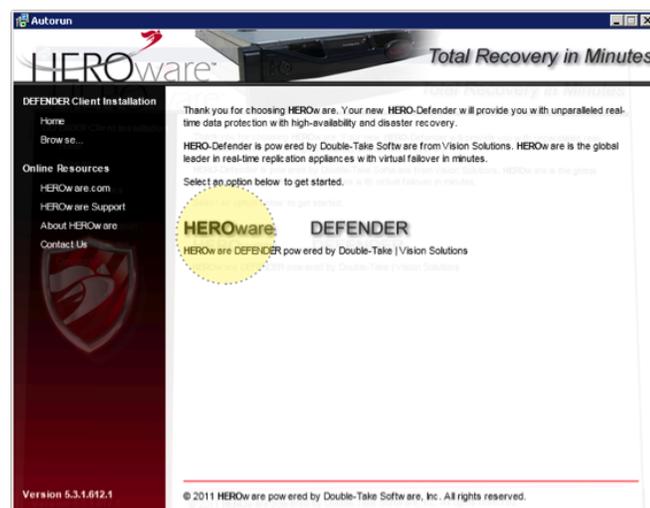


*Note: When installing Double-Take® for the first time and you did not complete the prerequisites, Double-Take will attempt to install .NET 3.5 and C++ updates, after which you may be asked to reboot - if not reboot anyway and rerun the Double-Take® install file to complete the process.*

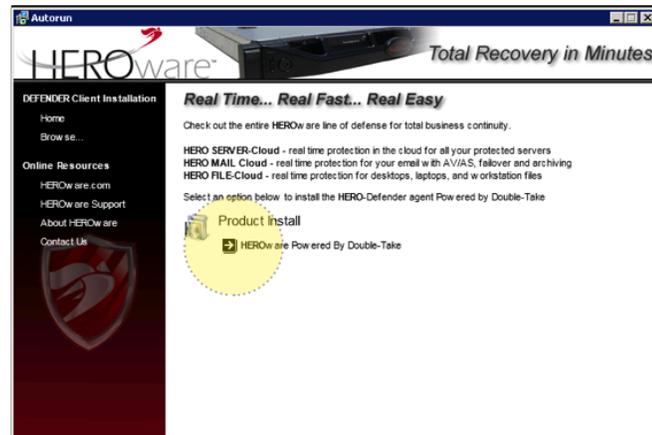
After prerequisites are complete the easiest way to manually install is to browse to the Defender's C: drive from the source and locate the Double-Take® install file (HeroDT...exe) and copy it to the desktop of the source. The Defender may require credentials if not a member of the domain. You can use the local Administrator with the password of "Heroware123". See path and file location below,



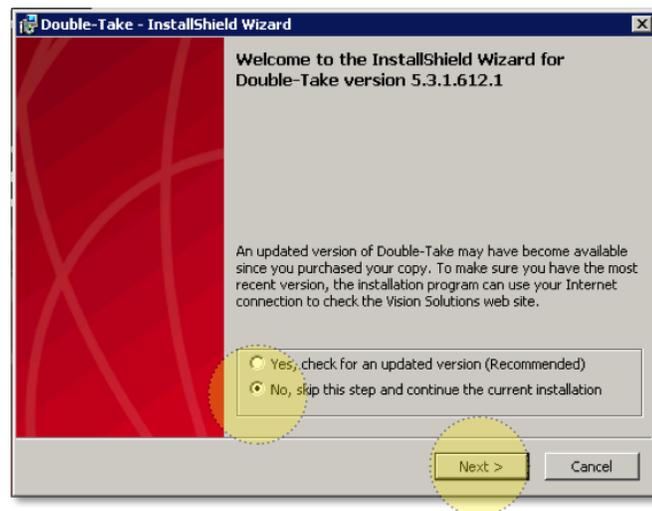
Now simply run the installation program and click on "HEROWare DEFENDER" then on the next screen click, "HEROWare...Powered by Double-Take®".



### Manual Client Installation continued...



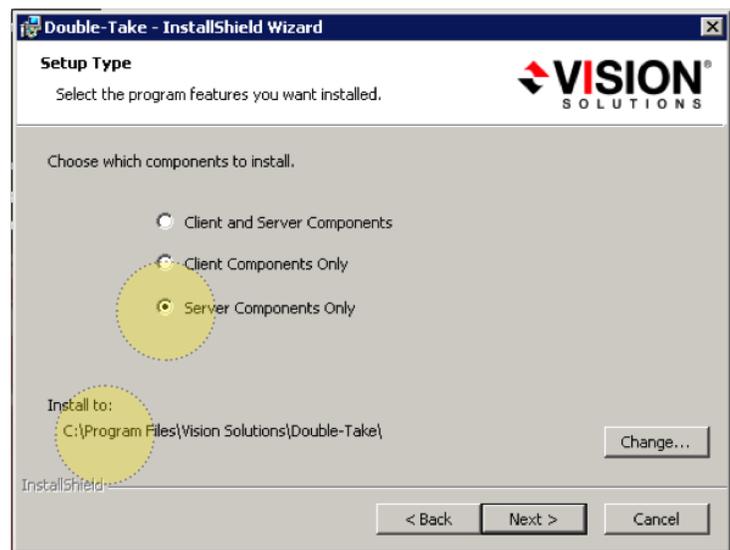
When you are prompted to update the software select “No” and Next, accept the license agreement and Next again.



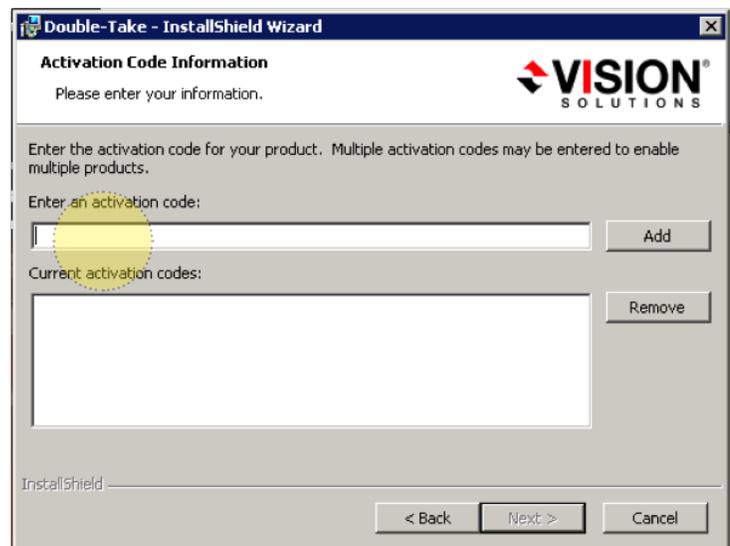
There are two components when installing Double-Take®, Client and Server. The Client simply installs the Double-Take® console allowing you to configure and manage replication jobs. The Client does not require an Activation code and is a management console only. Since the Defender has the console loaded there is no need to install the Client on or any of your source(s) except if you are looking for an alternate management console. The client is small and enables the Defender’s Double-Take® Console communications and configurations to the source(s).

### Manual Client Installation continued...

When prompted, select “Server Components Only” and for the program location- you can leave the default. Only change this location if you are running low on C:\ disk space.

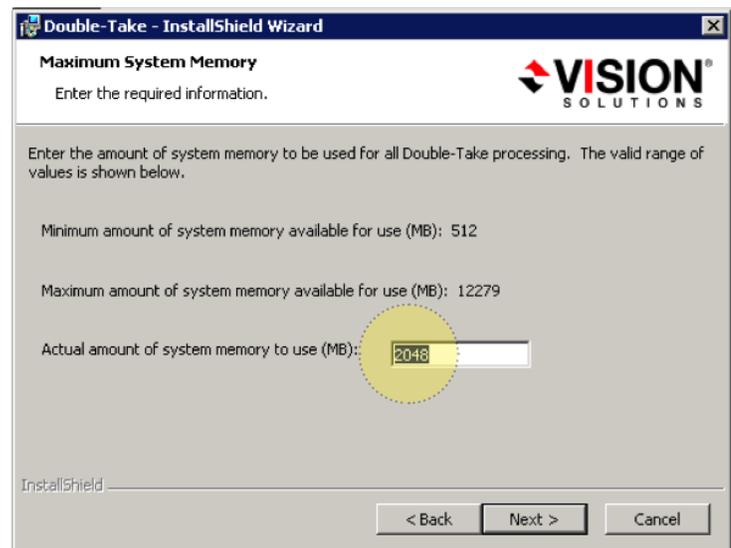


You should have received an Activation Code through email after your purchase of the Defender appliance. If you are unable to locate your Activation Code contact HEROware Sales or Support. Activation Codes have to be unique for each source and Defender to properly replication. Duplicate code will cause the replication job to fail.

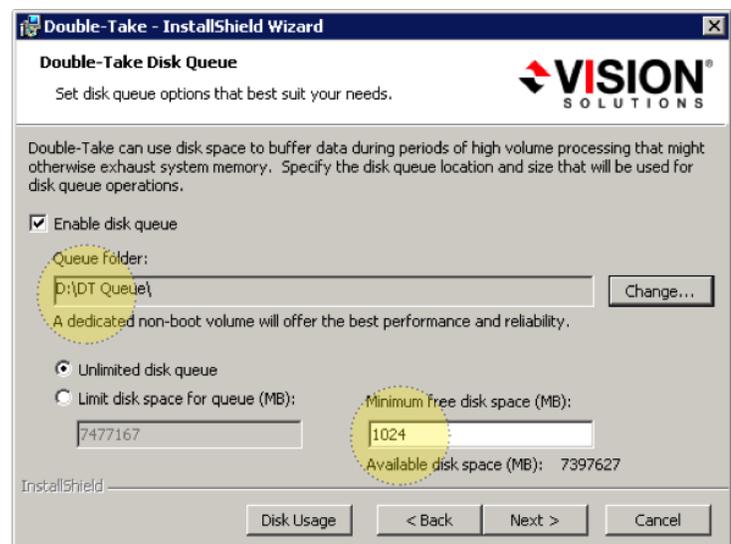


### Manual Client Installation continued...

Next; if your source OS is 64BIT and resources are available set Actual System Memory amount to 2048 (MB). This will help Double-Take® read/write operation quicker rather than cache them to disk.

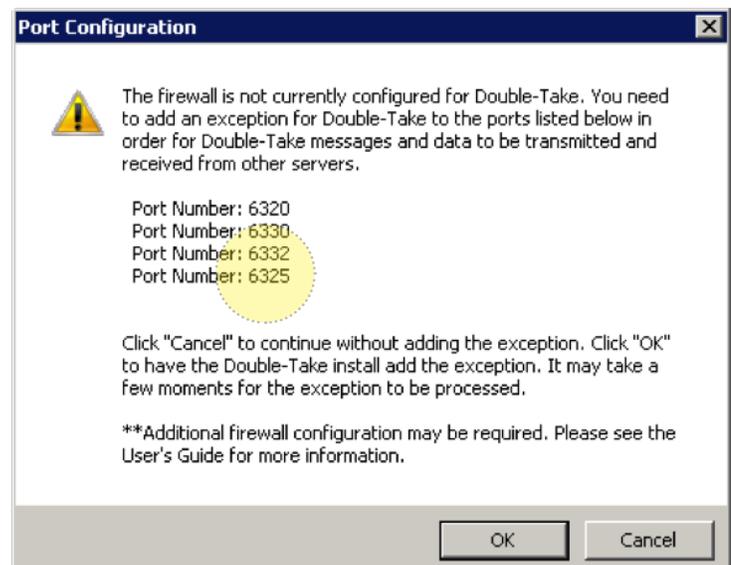


Using disk Queuing will help when other application(s) may be using resources. We suggest placing the Queue on a disk other than the boot partition. In this example we were using drive D:\. Set the minimum free disk space to 1024 (MB). If you are forced to use the boot partition set free disk space to 2048 (MB).



### Manual Client Installation continued...

Continue to take the defaults and install Double-Take®. When you come to the Port Configuration screen you are notified that Double-Take® requires four ports to be opened in order to operate. The installation process will attempt to create exceptions in the Windows firewall. As long as you are logged in with the proper credentials the exception should be created.



After selecting “OK” Double-Take® will continue to install. This process can take up to several minutes so please be patient. Once completed, click “Finished” and exit out of the HEROware Installer. Any temporary installation files will be cleaned and you are now ready to add the server to the Double-Take® Console on the Defender. See, “Adding a server to the console” in the TOC.



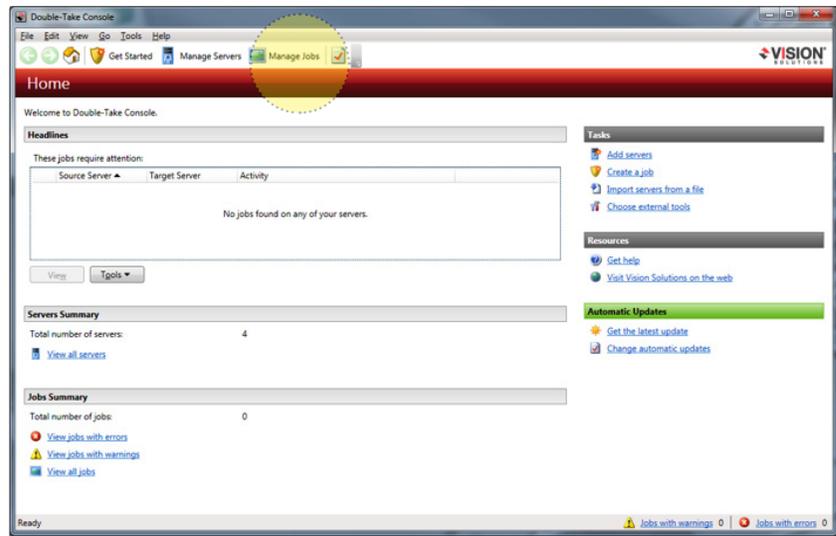
*Important: Once you have completed installation of Double-Take® it is strongly recommended that you create a domain user to use for replication credentials. This user needs to be a domain admin and the password should not change. Once the user is created add them to the local groups on the source server where you just installed the Double-Take® software.*

*Member of local groups:*

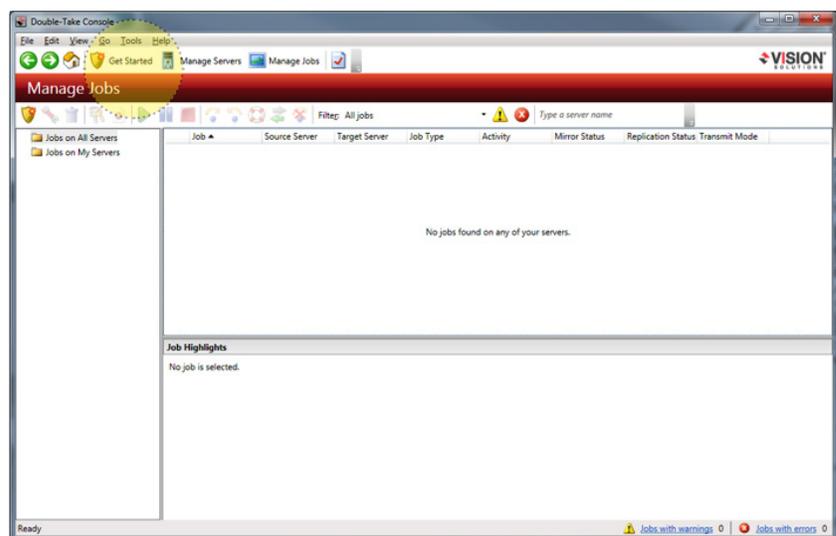
- *Double-Take Admin*
- *Administrators*

## Configuring a Replication Job

To create a Double-Take® replication job launch the DT console from **“Start\All Programs\Double-Take”** and select **“Manage Jobs”** from the top menu.

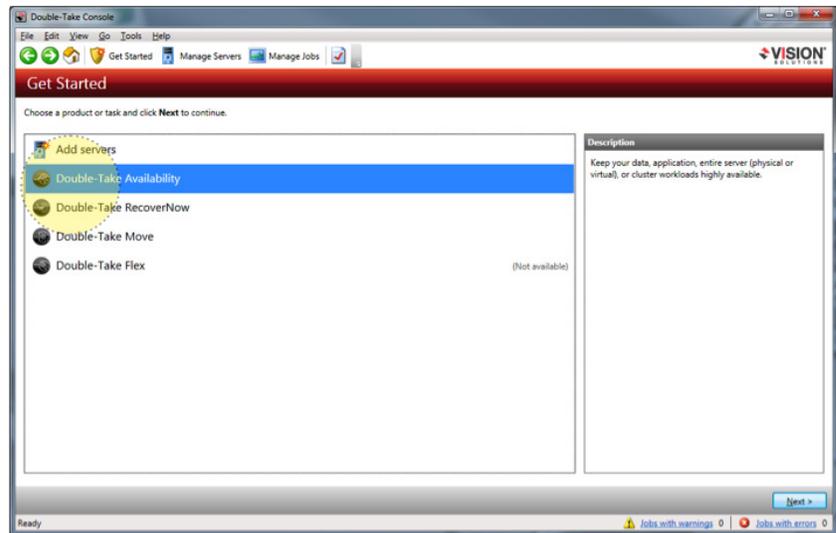


You can easily see what section you are in within the red bar across the top. As show in the image below you are in **“Manage Jobs”**. To begin a new replication job select the **“Getting Started”** shield in the top menu.

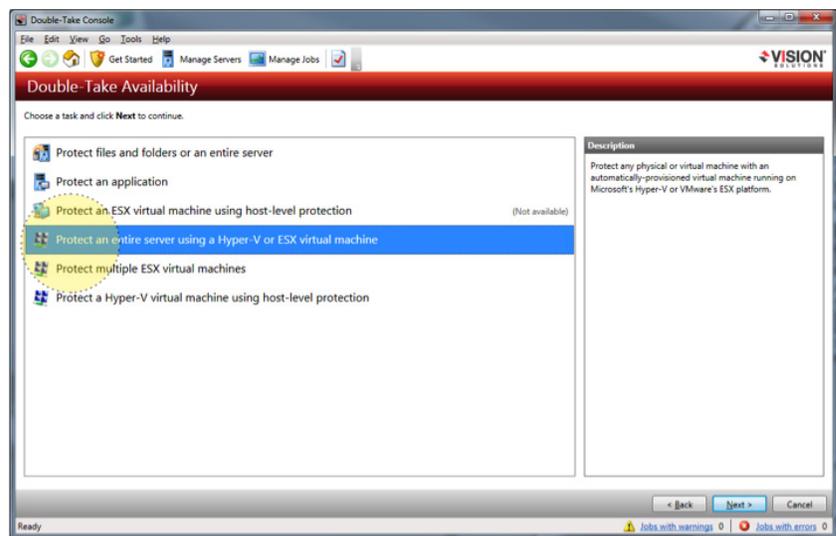


### Configuring a Replication Job continued...

Select “Double-Take Availability” under add servers,



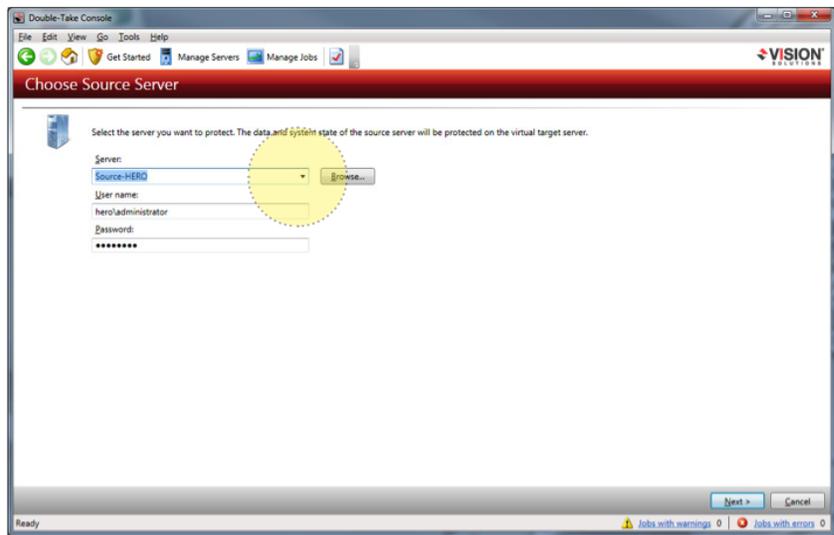
Select “Protect an entire server using a Hyper-V or ESX virtual machine”



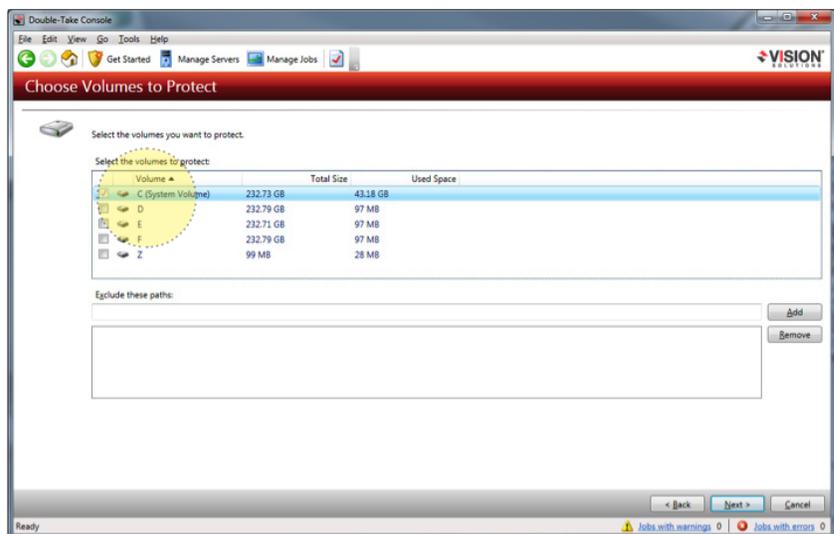
### Configuring a Replication Job continued...

From the drop down menu select a source server. A source server is a server you want to protect. If the server you want to protect is not listed you'll need to reference "Adding a server to the console" in the TOC.

Once the source server is selected it will automatically populate the credentials, click Next.

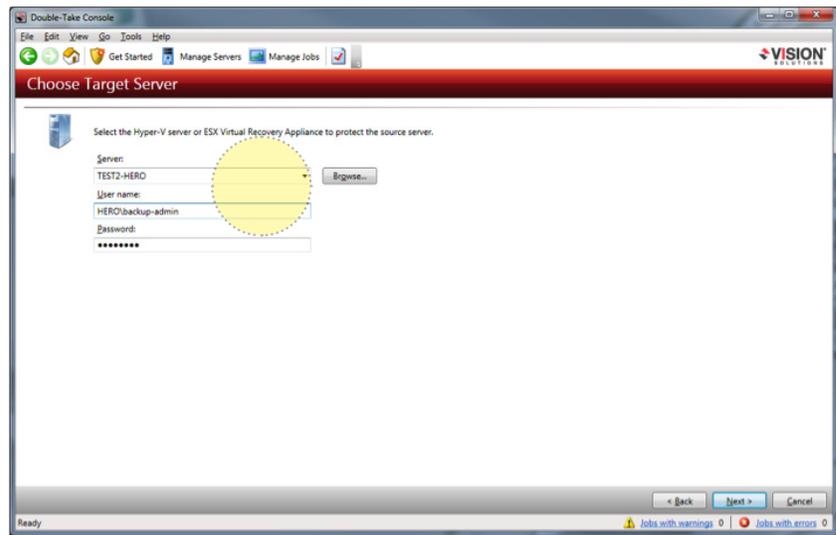


Choose what volumes or drives you want to protect. Also add any folders or files you would like to exclude, click Next.

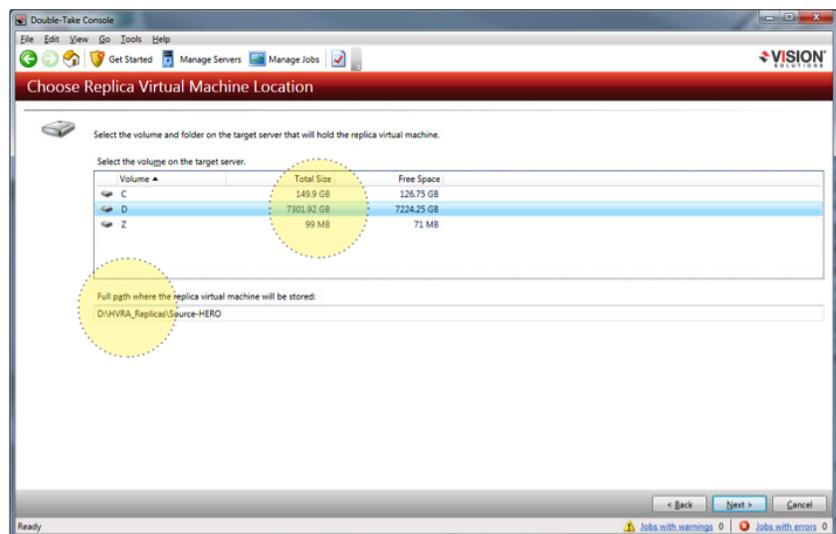


### Configuring a Replication Job continued...

From the drop down menu select a target server. A target server is the Defender running Hyper-V. Credentials will auto populate then click Next.



Once the connection is made a list of available storage space on the target (Defender) is displayed. Standard Defenders are shipped with an OS partition drive C:\ and a storage partition drive D:\. Select the storage partition, in this case drive D:\. Notice the full path folders structure is listed below. Click Next.

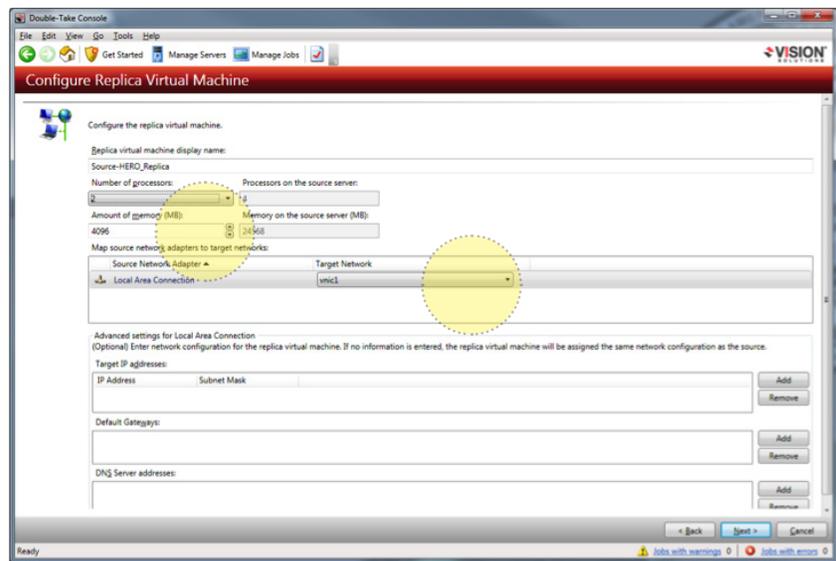


### Configuring a Replication Job continued...

When configuring the virtual machine the Defender will attempt to match the resources on the source, processors and memory. Notice that in the right column under the replica name will show available resources on the Defender.

It is recommended you build your virtual machine with minimum of 2 processors if multiple are detected and 4096 (MB) or 4GB of memory. Next to the “Local Area Connection” window your target network should have the virtual net adapter automatically selected. If this is not showing please use the drop down to select your vnic.

You can modify the processors and memory after the replication is complete if needed.



*Note: vnic or Virtual Network Adapter is configured using Hyper-V manager. If you're Defender was provided by HEROware your vnic has been preconfigured and will show up in the list. If you are using Defender Plus and provided your own hardware it is necessary to configure your virtual network adapter prior to configuring your job. See Microsoft® configuring a vnic for Hyper-V.*

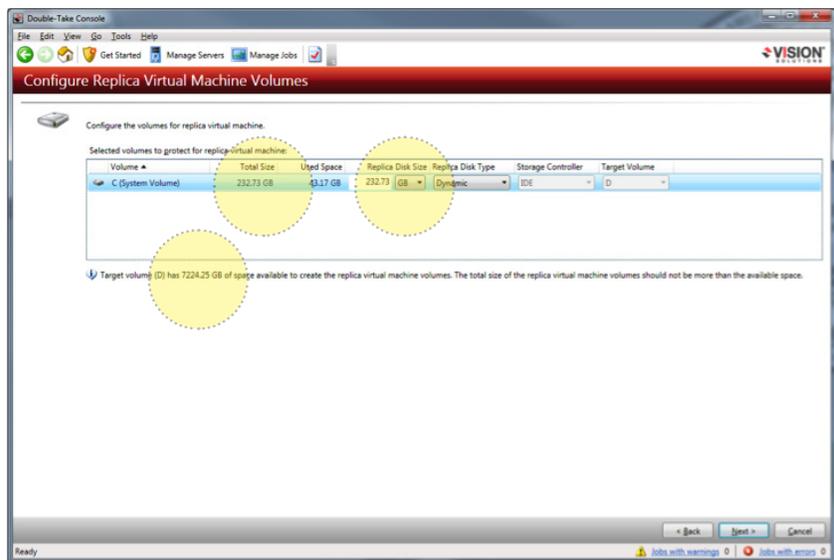
For best performance all other fields are best left alone.

### Configuring a Replication Job continued...

Now Double-Take® will build the VHD and match Replica Disk Size to equal the volume being created or Total Size. It is recommended that these two variables remain unchanged. (RDS) Replica Disk Size can be altered only in the event if the Target volume does not have sufficient space. If this is the case then the RDS can be modified to complete the job.



*Note: If you modify the RDS to accommodate the space on the Target volume and the Used Space grows larger than the RDS the VM will stop replicating. If the RDS has been modified its recommended you increase available disk storage space on the Defender then recreate the VM using the appropriate space suggested.*



Additionally the VHD defaults to Dynamic Disk Type. Leave this setting as Dynamic and Double-Take® will create a VHD to match the size of Used Space and allow the VHD to grow to the RDS. This will help when creating multiple replication jobs on the same volume.

### Configuring a Replication Job continued...

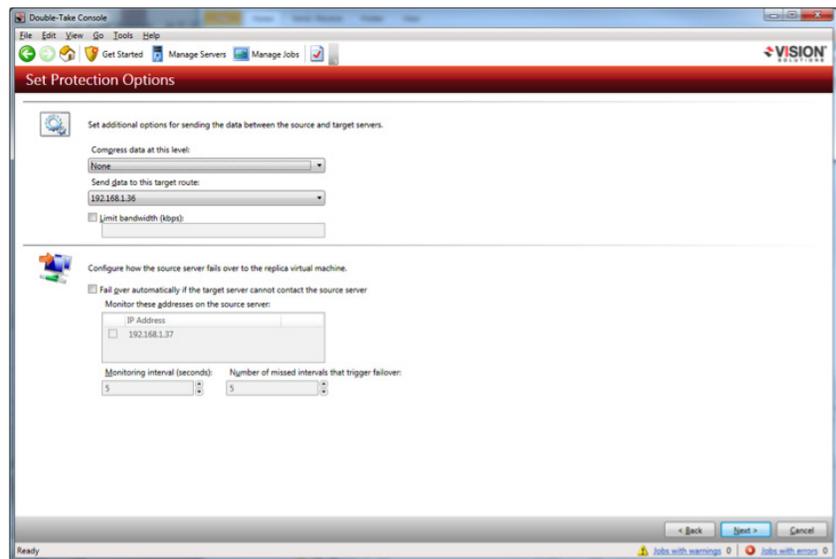
Leave these variables set to default. Compression should be enabled if replicating across a WAN.

The sent data target route reflects the primary IP address on the Defender. To check the IP address is correct run a ping test by name to the Defender.

Limit bandwidth is used when replicating across a WAN or the resources on the sources are low.

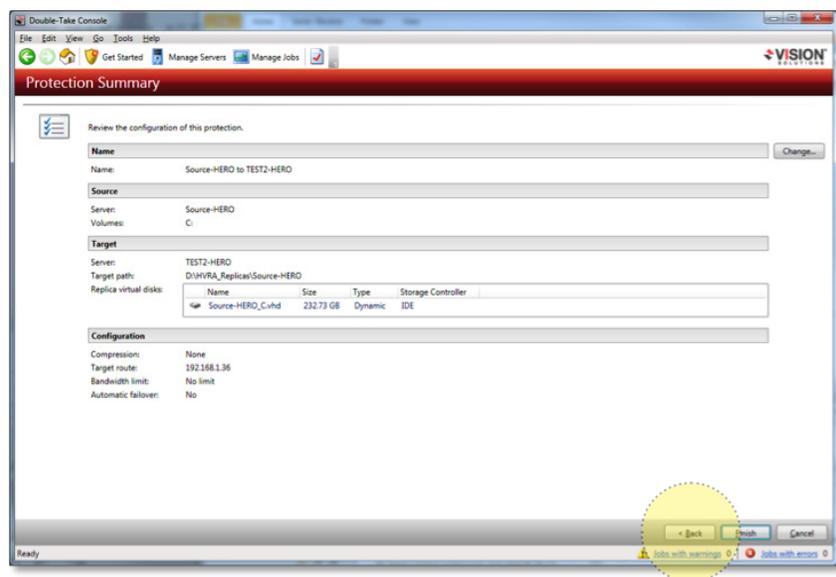


*Note: It is recommended NOT to set the job to automatic failover. If the replication job is set to automatically failover you must pay close attention to intervals and trigger so the Defender will not failover in case of a Patch or temporary reboot.*



### Configuring a Replication Job continued...

The last screen simply shows a summary of the configured replication job. Review your parameters and confirm everything is set per your input. If you need to modify any settings use the "< Back" button to correct them.



If everything is correct then click Finished and you will be taken back to the Manage Jobs screen where your newly configured job will show. The Manage Jobs screen will display replication status on all jobs noted under the Activity column. If you draw your attention to your newly created job the Activity column will go through a few different notifications while the job is building like, Connecting to Double-Take, Initializing VHD, Calculating, and finally Synchronizing (0.0%). Synchronizing shows you the progress by percentage. This could take anywhere from 20 minutes to 3 or 4 hours depending on network traffic, source server resource utilization, or used drive space on the source. Once the server is fully replicated the activity column will display Protected and there's a green circle check mark in front of the job.

**Configuring a Replication Job continued...**

Again note the Activity column during the replication process and the job warning indicator in Figure "A" and after completion in Figure "B".

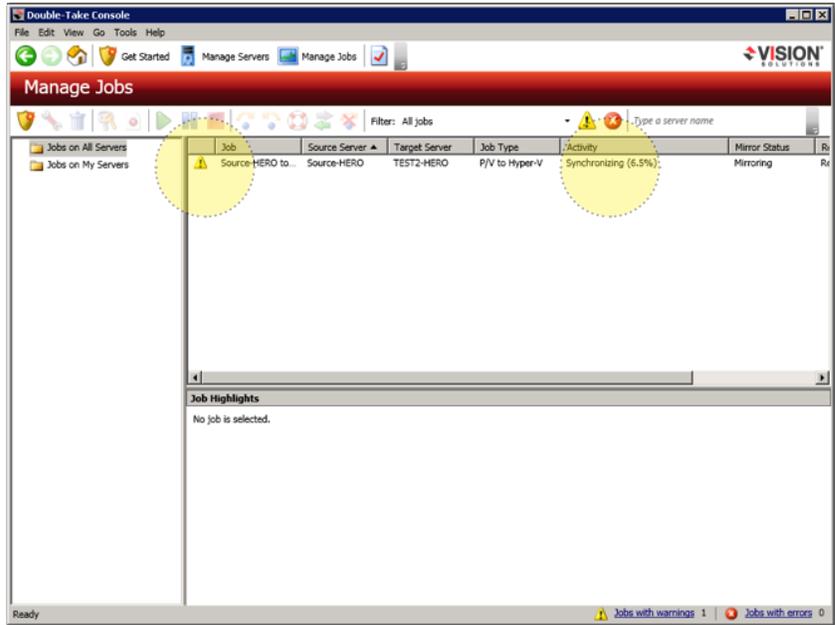


Fig. A

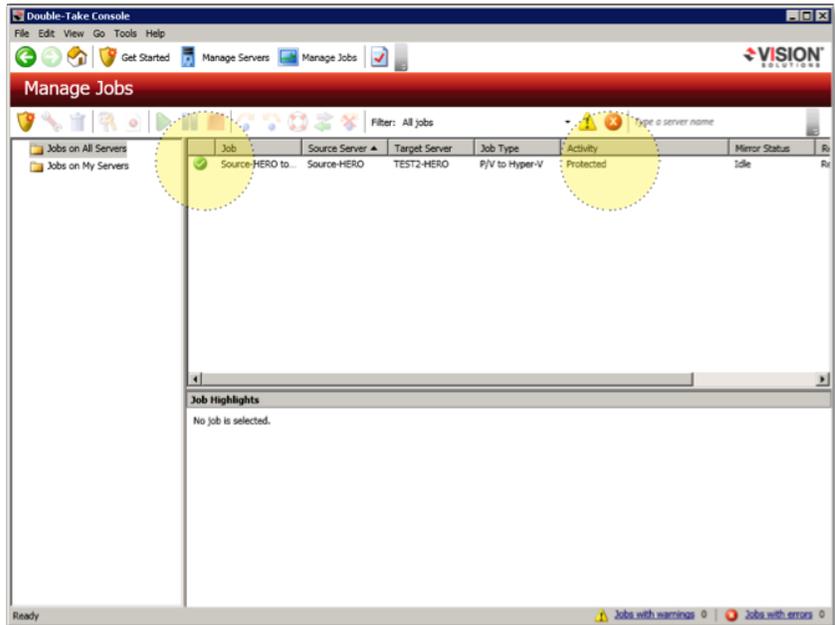


Fig. B

## Double-Take® Preparing and Executing a Failback

This section will help you prepare for and execute a Failback to a new or repaired server. It is not part of the initial set-up. In the event that you need to perform a live failover on the Defender, the replication job in Double-Take® becomes null. This is because Double-Take® has completed its task by replicating the source and spinning up the VM replica when the source failed.



*Note: Double-Take® is a tool used to interface between Microsoft Hyper Visor and your production server (source). Double-Take® automates the process based on variable inputs to create a Virtual Machine in Microsoft's Hyper Visor and continues to sync the production server with the VM in real time. Every job created in Double-Take® has its unique responsibility and when completed (failed over) it becomes null and can be removed from the Manage Jobs menu.*

Once the protected server has become inaccessible and you performed a live Failover, the Double-Take job in Manage Jobs menu should be deleted. When planning to Failback, you need to create a Files and Folders job to begin the process.



*Note: Remember because the Defender is now hosting your production server virtually, your users are not interrupted and productivity continues to happen. Now you have the luxury of planning the Failback on your time.*

### Configuring a Files and Folders Job

A few things need to happen before you build the Files and Folders job. Concerning the physical production server that has gone down.

#### Identify and fix any hardware problems on the physical server

- You can use this time to add additional drive space or memory if needed.
- When recreating any drive partitions it's important to duplicate the original partition configuration. You can add to the partition configuration but it is not recommended to subtract.

#### Re-install your server OS

- It is recommended you install the same version of server OS.
- Only install standard if reinstalling SBS server. The F&F job will reconfigure the server to SBS once the job is activated.
- Leave the IP address dynamic and server name generic. The F&F job will take care of renaming and addressing your Failback.

### Configuring a Files and Folders Job continued...

Below shows a configuration example needed in preparation for a Failback job. Notice the production server parameters match or exceed the virtual machine parameters. As mentioned previously it's important not to exclude partitions or shirk disk size on the physical or target server when preparing for a Failback.



Defender



Physical Server

#### Virtual Machine

Microsoft: 2008R2  
Memory: 2048MB  
Processors: 1CPU  
NIC: 1  
Drive C:\ (150GB)  
Drive D:\ (1.5TB)  
Drive E:\ (800GB)



#### Production Server

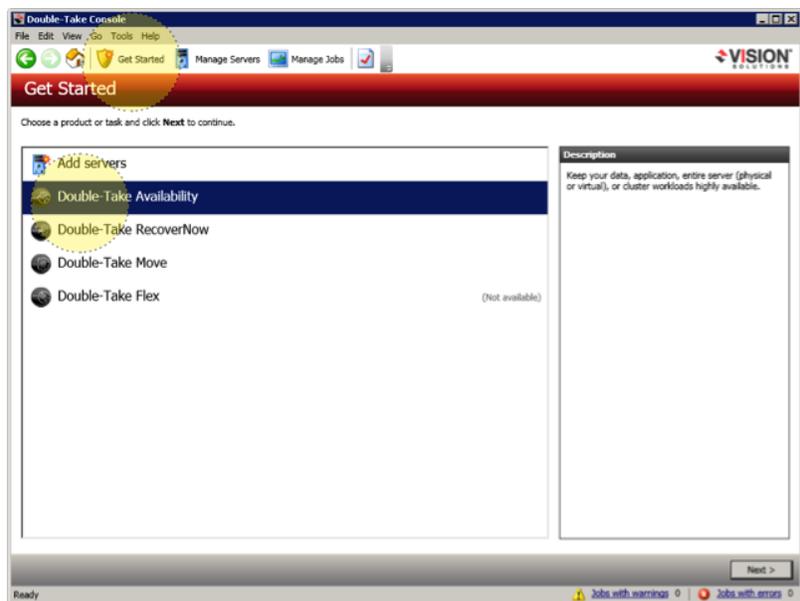
Microsoft: 2008R2  
Memory: 4096MB  
Processors: 2CPU  
NIC: 1  
Drive C:\ (150GB+)  
Drive D:\ (1.5TB+)  
Drive E:\ (800GB+)  
Drive F:\ (ok to add)



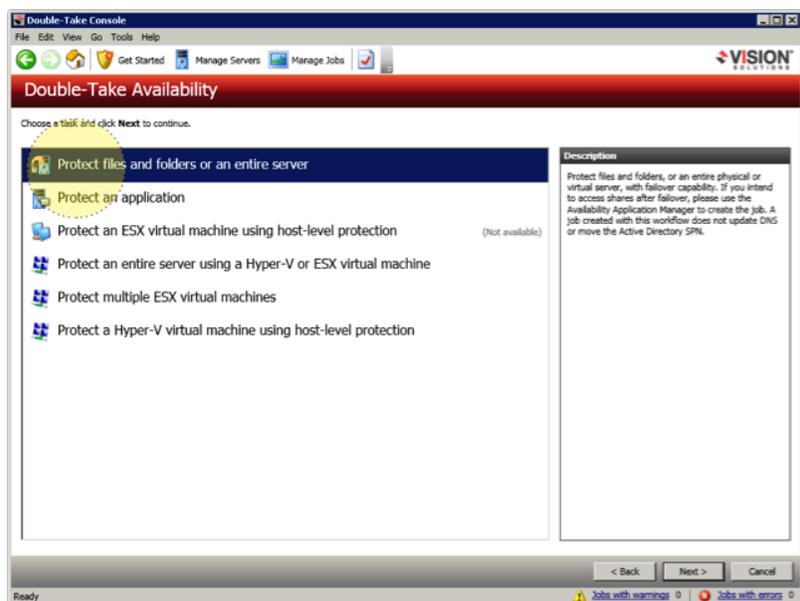
*Note: unlike a replication job, the physical server or repaired server becomes the target and not the Defender. In summary the VM running on the Defender is the source and the physical server becomes the target.*

### Configuring a Files and Folders Job continued...

To create a Files and Folders job launch the Double-Take® console on the Defender and make sure both servers (Source and Target) are listed and authenticated under Manage Servers. If not listed see adding servers to the console in the TOC. After verifying servers select “Get Started” on the top menu of the console then select, “Double-Take® Availability”.

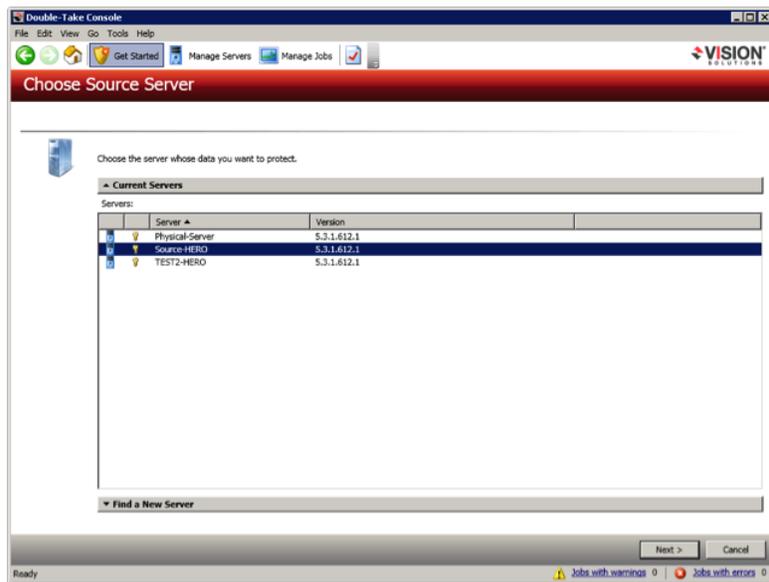


Next select, “Protect files and folders or an entire server”

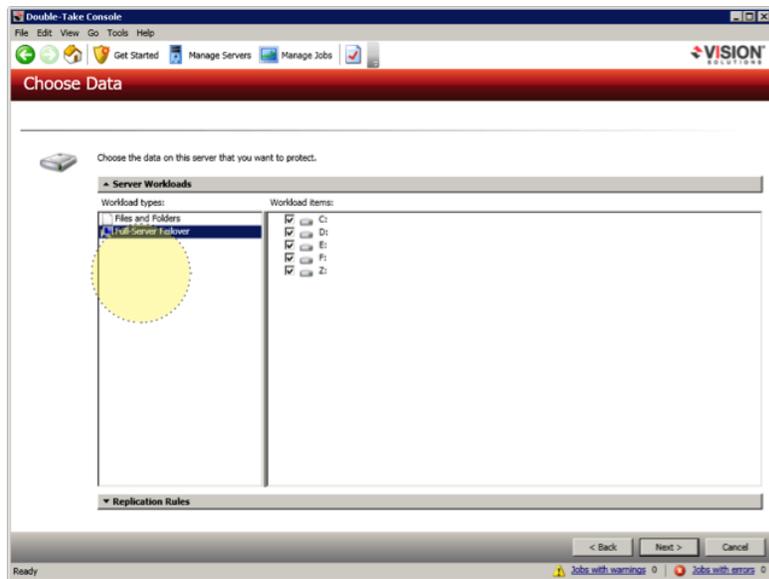


### Configuring a Files and Folders Job continued...

“Choose Source Server”, A list of all the servers added and authenticated is displayed. In this example Source-Hero is a VM running on the Defender and our source for failing back.

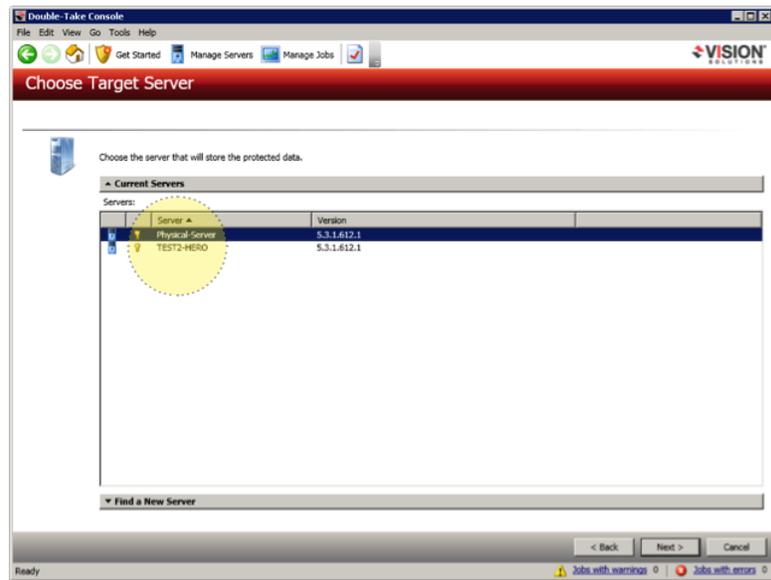


Next is “Choose Data”. The ability to select Files and Folders/Full-Server Failover are your two options. Remember that your target server should have drive partitions that match the VM source. Since we are creating a job to perform a Failback you will select “Full-Server Failover” and continue.

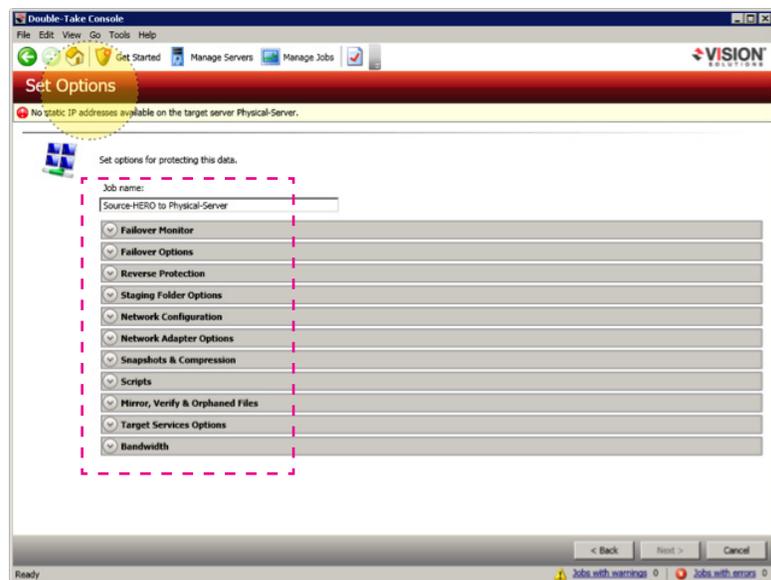


### Configuring a Files and Folders Job continued...

Now “Choose Target Server” is the physical server you just fixed and you will be failing back to. For this example we are selecting “Physical-Server”.



Your next screen is the “Set Options” screen and has a variety of variables in multiple categories that can be configured. Most of the setting are preconfigured so we will just address the categories of concern. If you see a No static IP address available... banner under the set options bar it's no concern. The target IP will reflect the source once the failback is complete.



### Configuring a Files and Folders Job continued...

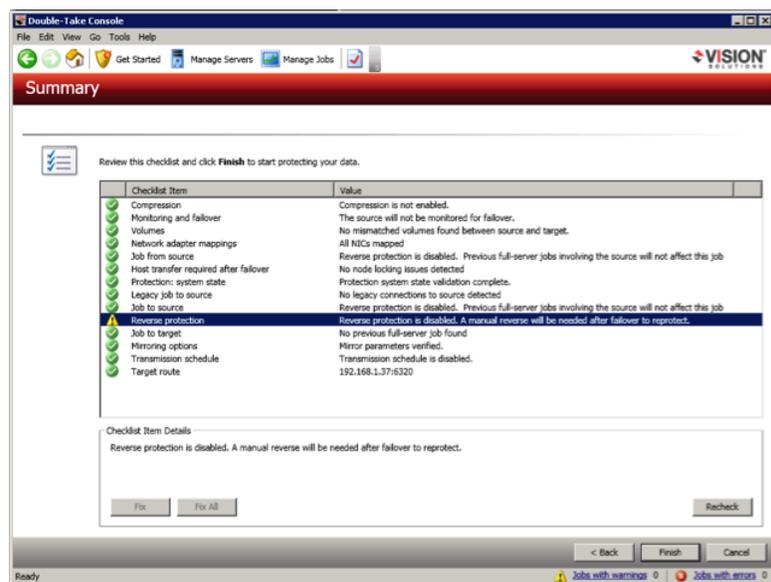
Set Options;

1. Failover Monitor – preconfigured with Source IP.
2. Failover Options – preconfigured with “Wait for user to initiate failover”.
3. Reverse Protection – select: “Disable reverse protection”.
4. Staging Folder Options – left blank.
5. Network Configuration – preconfigured with “Apply source network configuration to the target...”.
6. Network Adapter Options – left unchanged.
7. Snapshots & Compression – uncheck “Enabled scheduled snapshots”.
8. Scripts – left unchanged.
9. Mirror, Verify & Orphaned Files – select “Mirror all files” leave the rest unchanged.
10. Target Services Options – left blank.
11. Bandwidth – left unchanged. (Recommended)

Once you complete the next screen “Summary” will check your variables and flag any conflicts or concerns. They can be corrected using the back button.

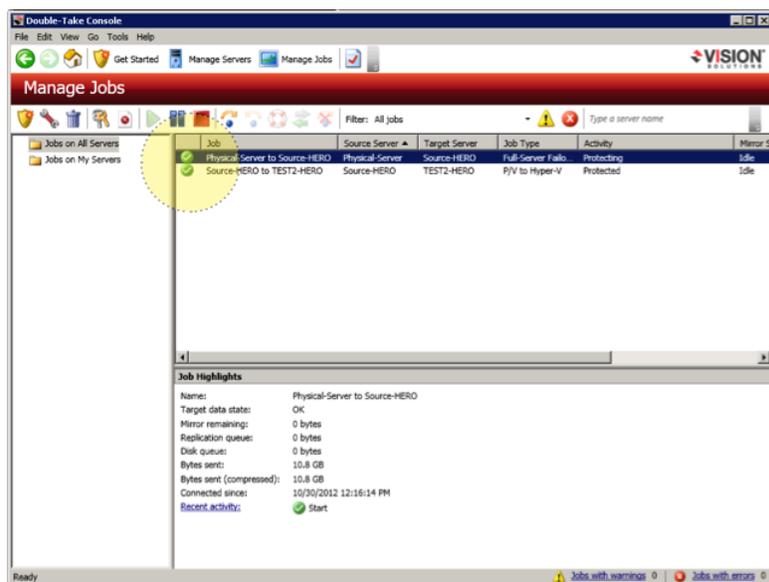
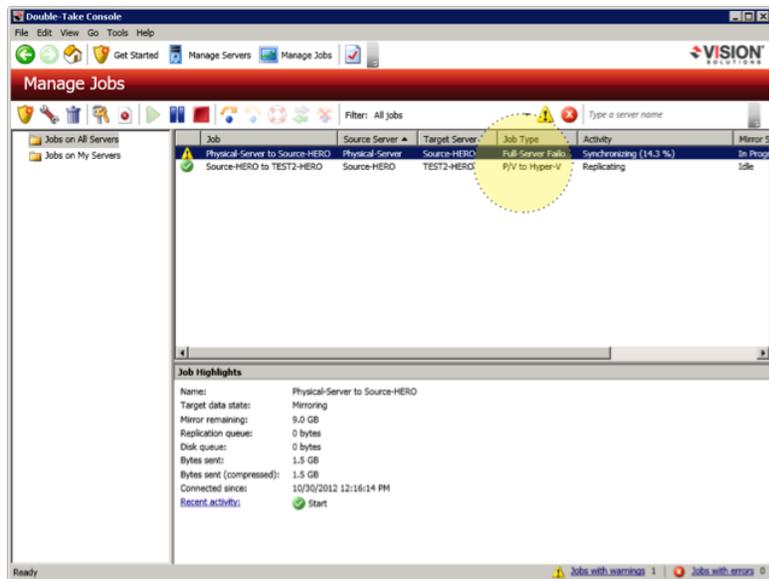


*Note: Make sure you pay attention to the flags. Not all flags need to be corrected rather they may just be for your information. Example, if you added more processors or disk space to the target you'll be flagged that these variables do not match. In this example reverse protection has been disabled.*



### Configuring a Files and Folders Job continued...

After you corrected and or satisfied with your configuration you'll select finished. Then the Manage Jobs screen will show your new job listing and begin to synchronize the servers. Notice that unlike your real-time replication jobs this job is flagged as a "Full-Server Failover". Once completed the status with display the same as your other jobs with a green check circle to the left indicating it's fully protecting.





---

## **HEROware, Inc.**

65 Enterprise, Aliso Viejo, CA 92656

P (866) 810-4376

[www.heroware.com](http://www.heroware.com)

Last updated: 10 May 2013

© 2013, HEROware, Inc. All Rights Reserved.