WANSyncHA® Microsoft IIS Server™

WANSyncHA Microsoft IIS Server Operations Guide

Contents

Appendix C: Move IP Redirection

Appendix D: Switch Computer Name Redirection

Appendix E: Replication in a Workgroup Environment

Index

Chapter 1: Getting Started

WANSyncHA IIS is a Microsoft IIS web server switchover solution based on asynchronous real-time replication and automated application switchover and switchback to provide cost-effective business continuity for Microsoft IIS on both 32- and 64-bit Windows servers, as well as MSCS clusters.

WANSyncHA offers push-button or fully automatic switchover of mission-critical web, FTP, NNTP and SMTP servers over a LAN or WAN, IIS-aware status monitoring, integrated continuous data protection as a guard against data corruption, and completely non-disruptive automatic testing of your IIS disaster recovery system, all in a system that sets the standard for ease of configuration and management.

About This Guide

This document is a guide to implementing a high availability solution for Microsoft IIS Server 5 and 6, based on WANSyncHA replication to a remote secondary server with automated switchover and client redirection.

Please review each procedure before starting, in order to ensure you have the appropriate resources and permissions to carry it out.

Related Documentation

Use this guide along with the *WANSync User Guide*.

Requirements

This section describes the requirements for running WANSyncHA for Microsoft IIS server.

Infrastructure

To implement high availability with WANSyncHA for Microsoft IIS Server, you must have/implement the following:

- Two servers running Windows Server 2000 or 2003
  - Both servers should have the same level of service packs and hot fixes installed
- An instance of Microsoft IIS Server 5 or 6 installed on each server
  - Both servers should have the same IIS services installed: WWW, SMTP, etc.
  - Both servers should have identical web service extensions installed
  - Full paths containing site files should be identical on both servers
- The passive server should hold a clean installation of IIS with the default sites only
- Sites on the master server should not use URL redirection or UNC path redirection
- If anonymous access is enabled and used, configure the following:
  - In order to keep permissions synchronized between the two servers, both IIS processes should use the same user account for anonymous user access. Create a new domain user account and configure both IIS servers to use it. The following articles describe how to do this:
  - **For IIS 5.0**: *How To Configure IIS 5.0 Web Site Authentication in Windows 2000* http://support.microsoft.com/kb/310344
  - **For IIS 6.0**: *How To Configure IIS Web Site Authentication in Windows Server 2003* http://support.microsoft.com/kb/324274
  - Please note that although the article does not specify it, it is required to edit the local (or domain) group policy to allow the user account the following privileges: Allow log on locally, Allow log on as a batch job, and Access this computer from the network. Also, make sure to duplicate any permissions changes made to the file system for the original anonymous user account to the newly assigned domain account as well.
- In IIS 6.0, if you define any new Application pools on the master server you should also define them on the replica server
- If you are using SSL encryption, please see the following MS article concerning copying the proper certificate: *How to load balance a Web server farm by using one SSL certificate in Internet Information Services version 6.0 and in Internet Information Services 5.0* http://support.microsoft.com/kb/313299
- Statically assign all IP addresses (DHCP-assigned IP addresses on the master or replica server are not supported)
- The protected server is not a domain controller or DNS server

Log On Account

The WANSyncHA service log on account must satisfy all of the following account conditions:

- It is a member of the Domain Admins group. If the Domain Admins group is not a member of the built-in domain local group Administrators you must use an account that is.
- It is a member of the local machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

  Important! If your company's security policy requires more granular permissions than described, please contact technical support to receive detailed instructions. Special considerations apply to IIS servers operating workgroups: see *MS IIS Servers Operating in a Workgroup*.

Non-Intrusive Installation

During installation and configuration of WANSyncHA, Microsoft IIS Server on the master server continues working without any interruption.

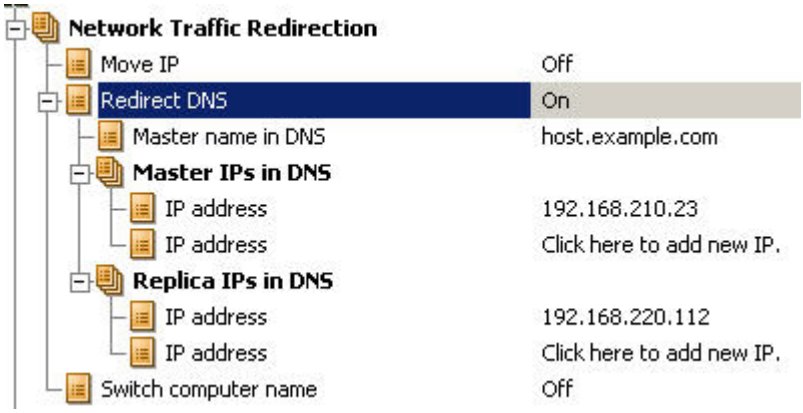
Determine Which Redirection Method to Use

There are four ways in which you can redirect clients after switchover: Redirect DNS, Move IP, switch computer name, and custom scripts. You can use each method alone or you can use them in any desired combination.

Important! If you will be redirecting File Shares, in which clients connect to via the master server name, switch computer name must be enabled. For example, if the master server's name is fs01 and clients connect to \\fs01\sharename or \\fs01.domain.com\sharename then you must use the Switch computer name method. It's also recommended to enable one other method as well. The most common method is to use both DNS Redirection and Switch Computer Name.

- **Redirect DNS**. Upon failure of the master, the replica server modifies the appropriate DNS record so that references to the master server resolve to the replica's IP address rather than the master's IP address. This solution is the easiest to implement and requires no network reconfiguration. DNS redirection works only with A (host) type records and cannot update CNAME (Alias) records directly. However, if the CNAME record points to the modified A record, it is indirectly redirected.

Using the record that has the master server's name is the default, however you can configure WANSyncHA to redirect any DNS A (host) record via the *Master's name in DNS* setting in the switchover properties tab.



- **Move IP.** This redirection method is usable only in a LAN configuration in which the master and replica servers reside in the same network segment. In this configuration, switchover of the master server causes the replica to take over one or more of the IP addresses assigned to the master server.

  If you want to use Move IP, please see *Move IP Redirection* before configuring the replication scenario.

- **Switch Computer Name**. If you are redirecting File Shares, in which clients connect via the master server name, enable switch computer name. For example, if the master server name is fs01 and clients connect to \\fs01\sharename or \\fs01.domain.com\sharename, use the Switch computer name method. It's also recommended to enable one other method as well. The most common method is to use both DNS Redirection and Switch Computer Name. WANSyncHA makes the required computer name switch by assigning a temporary name to the master server and taking over its computer name for use with the replica server: WANSyncHA updates records directly and does not generally require a reboot. If, however, you encounter any problems after switchover, consider setting the reboot option to On and testing again. For most cases, the reboot option is not required. Please see *Switch Computer Name Redirection*.

- **Custom Scripts**. WANSyncHA can trigger custom scripts or batch files to perform the user redirection or any additional steps not covered by built-in methods. If the above methods are not appropriate or do not fully meet all requirements, please see the *WANSync User Guide* for details on scripted redirection methods.

MS IIS Servers Operating in a Workgroup

For servers in a workgroup, set the XOsoft Engine service account to Local System (unless you have added any custom scripts that require higher level permissions). Servers in a workgroup can use Redirect DNS only with DNS servers that allow non-secure updates. You can use Move IP, switch computer name, and custom redirection scripts normally.

About MSCS (Shared Storage) Clusters

With WANSyncHA, installing on clusters is much the same as a standard installation. To install on a cluster, enter the IIS Server's Virtual Server Name as the master or replica name. You must also install the XOsoft Engine on all cluster nodes.

For detailed instructions on using Move IP with clusters, please see *Move IP Redirection* before configuring the replication scenario.

License Keys

When first opening WANSync Manager, it prompts for a license key. This key determines what scenario types and features are available. To simplify key installation, you can paste the entire key directly into the first text box. Subsequent text boxes are filled automatically. After opening the Manager, you can view and apply license keys from the *Help*, *About* menu.

WANSyncHA Components

WANSyncHA is comprised of the following components:

- **XOsoft Engine**. WANSyncHA's service - runs on each server involved in the scenario.
- **WANSync Manager**. Management GUI - used to manage and configure WANSyncHA.

XOsoft Engine

The XOsoft Engine is the executable file that lies at the heart of the WANSyncHA system. It is installed on every host participating in replication and must be running before any replication scenario can run. Each engine can act as a master or replica with respect to each replication procedure or *tree*. It can also participate in more than one replication tree, as long as the file system directories, to which the different replication procedures are applied, don't overlap one another. WANSyncHA communicates via default TCP port 25000 (you can change the default port number).

WANSync Manager

The Manager is a graphical user interface (GUI) application that controls all replication hosts, both in the definition and operation (running) of replication services. The offline process is mainly the definition of replication scenarios. Once a replication scenario is sent to the participating hosts, the Manager also provides the means for online control (running, synchronizing, etc.) and monitoring (i.e., node status, log files, etc.). You can operate the WANSync Manager from any location from which connections are established to WANSyncHA hosts.

Note: The Manager connects as a TCP client to master and replicas defined in the replication scenario. Once a replication process is running, the Manager is no longer required for the process to continue. Connection to replica hosts is not mandatory - it is required only in order to enable selection of destination directories via browsing, instead of manually. Connection to the master host is mandatory.

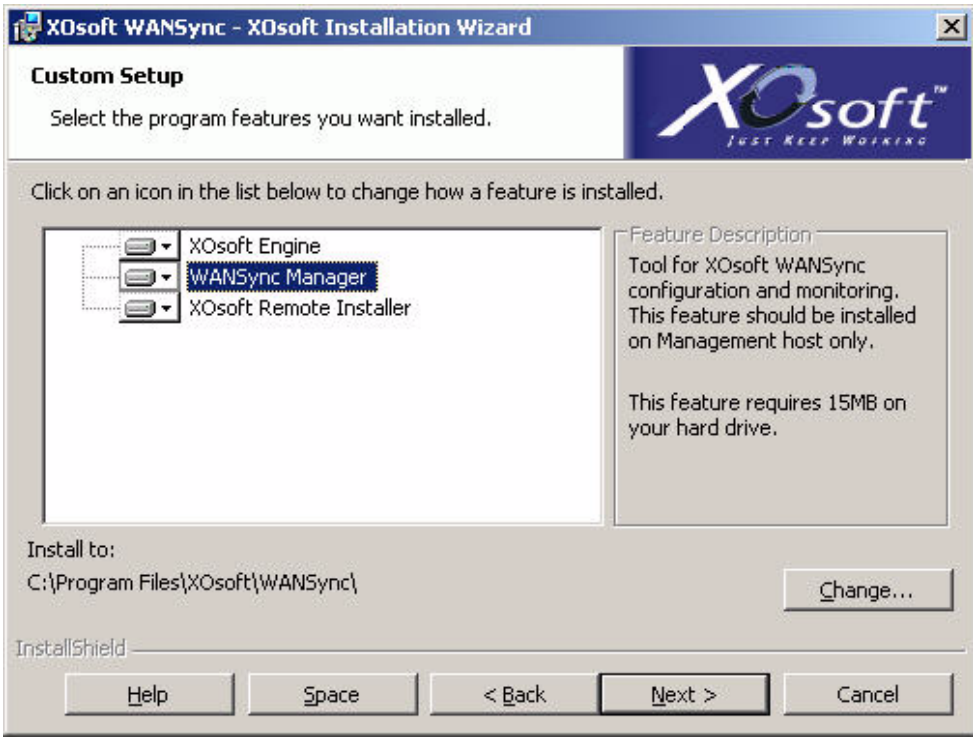
Chapter 2: Server Setup

This chapter describes the most common setup for WANSyncHA for IIS servers.

Install WANSync Manager

Install WANSync Manager and the Remote Installation Wizard onto the machine from which the WANSyncHA scenario will be configured. The location of the Manager is not critical so long as it is accessible in the event of a disaster. Frequently, the Manager is installed on an administrative workstation.

Note: If the Manager is installed directly on either the master or replica servers, ensure that the XOsoft Engine is also installed.



If you intend to use the XOsoft Remote Installer (recommended), the machine on which you are running the remote installer must have the .Net framework 2.0 installed. The framework is required only on the machine running the remote installer wizard (GUI); the target servers do not have this requirement.

After the scenario is run it is cached on your master and replica servers. Once cached, you can download it to any installed WANSync Manager by selecting *Download* from the File menu (then enter the name of your master or replica server).

Prepare the Servers

The following subsections describe how to prepare IIS servers for use with WANSyncHA.

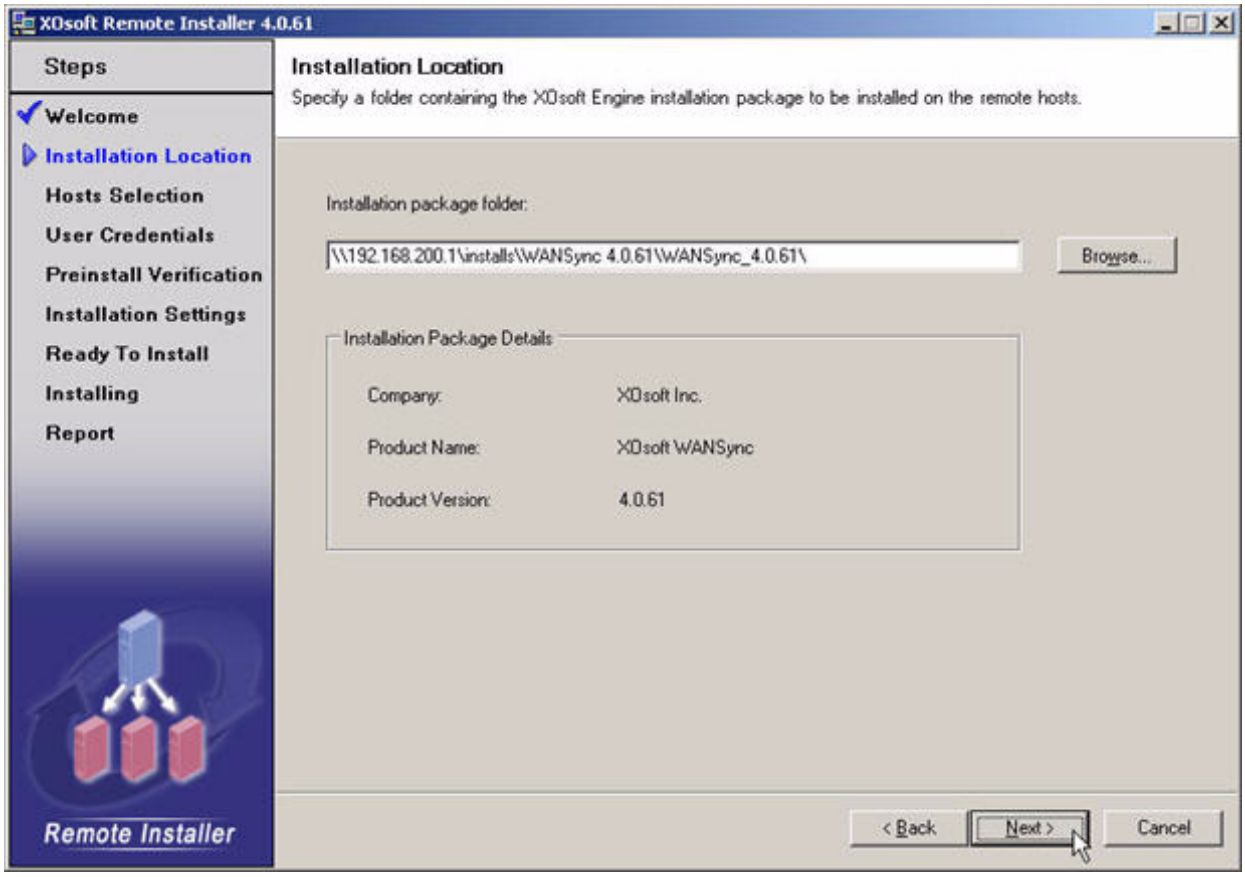
Remote Installation Wizard

You can use the Remote Installation Wizard to deploy the XOsoft Engine to any number of servers, or cluster nodes, in one step. Alternatively, you can install the XOsoft Engine manually by running setup.exe directly on each server.

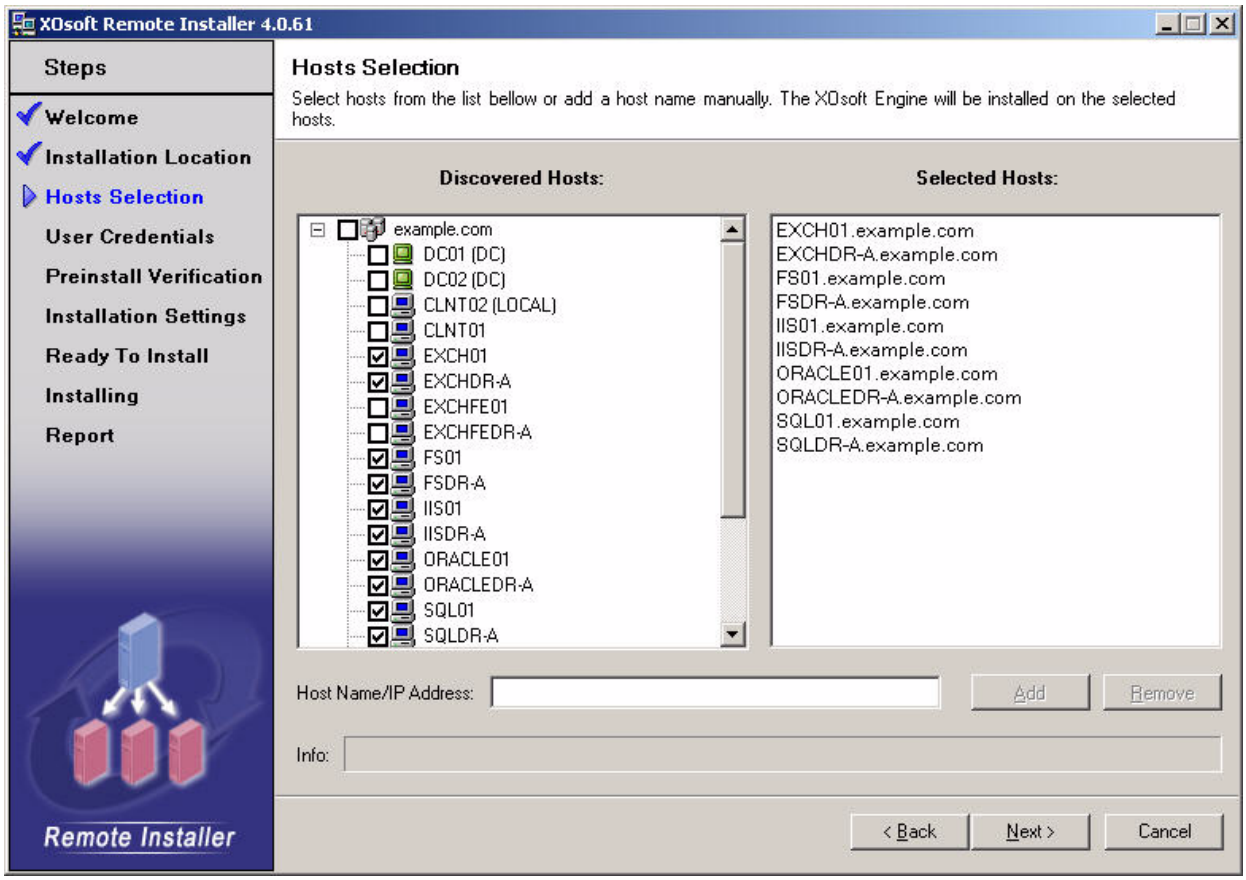
Note: If you install the XOsoft Engine using the remote installation wizard, you can skip the the manual installation step under the sections *Master Server* and *Replica Server*.

Run the remote installation wizard either from the start menu or from the WANSync Manager Tools menu. When using the remote installation wizard, consider the following steps:

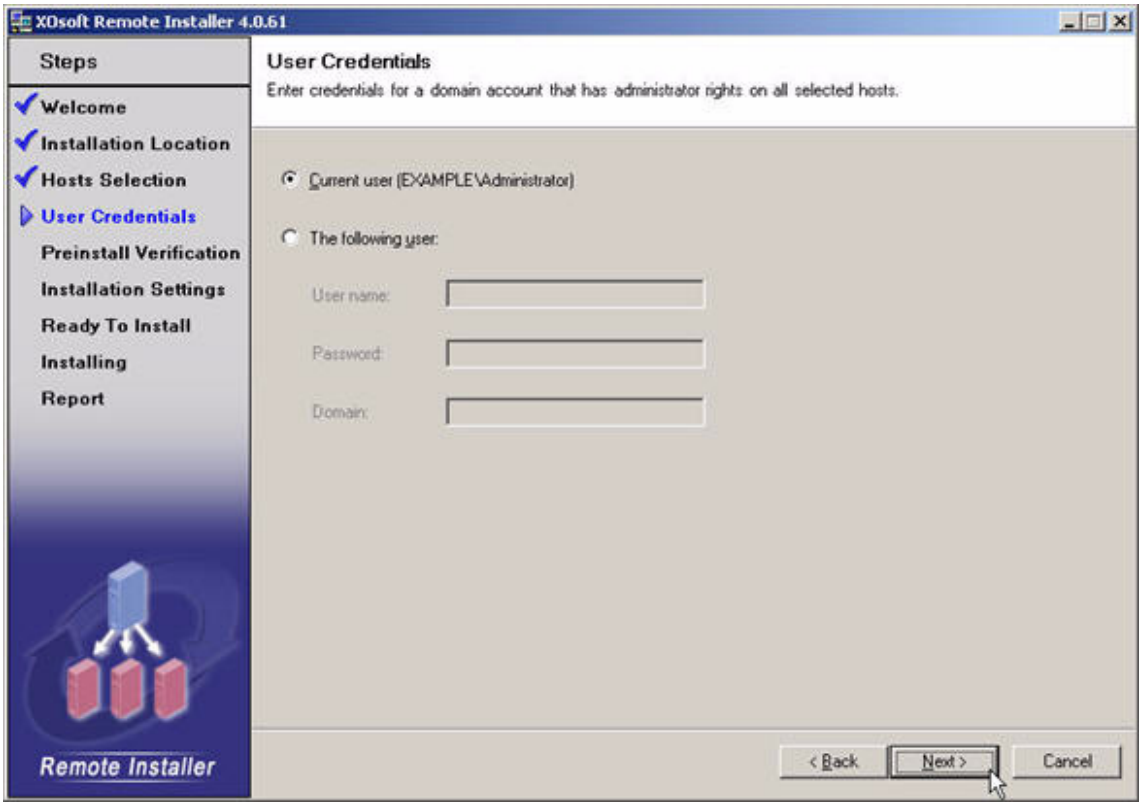
- **Installation location** - ensure that this path is correct and contains a valid WANSyncHA setup package



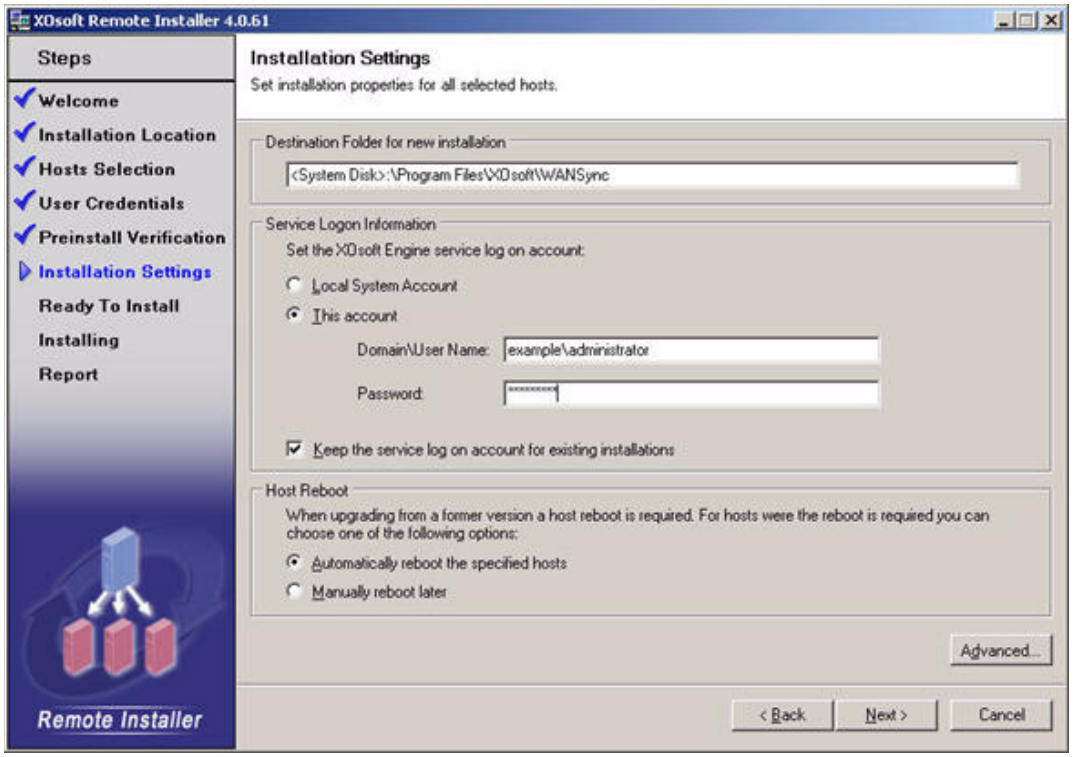
- **Hosts selection** - select the servers (or cluster) nodes to which you want to deploy the XOsoft Engine (you can add servers manually from the *Host Name/IP Address* box)



- **User credentials** - the user account that is used to install the XOsoft Engine on each target server (ensure that this account is a local Administrator on all target machines)

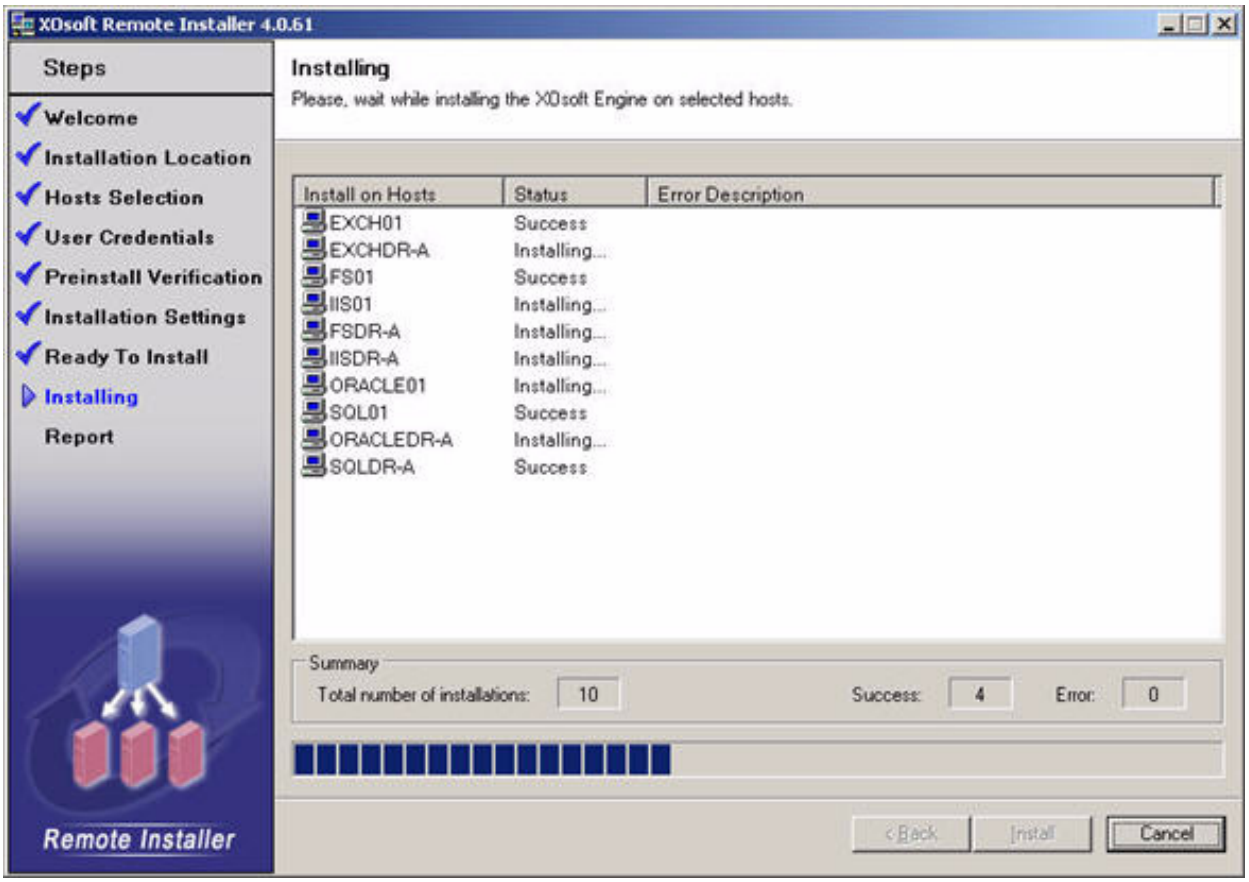


- **Preinstall verification** - click Next after all servers have reported success
- **Installation settings** - select *This Account* and enter the WANSyncHA service account domain\username and password (see *Requirements* for more details)

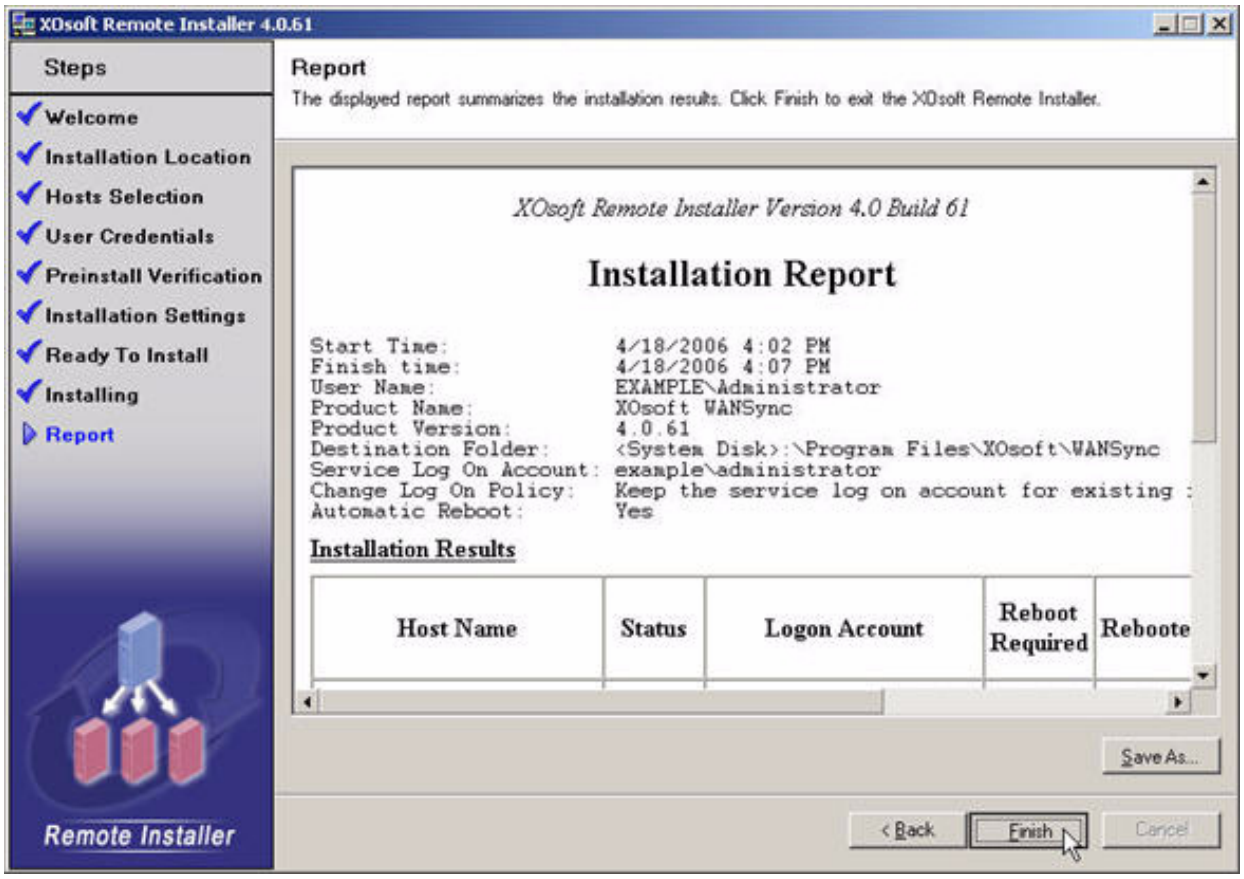


Note: Do not proceed without first setting the correct service account (see *Requirements* for more details).

- **Ready to Install** - confirm that all desired servers are listed and then click the Install button
- **Installing** - you can monitor the installation process from this screen



- **Report** - in this last step you can view the full installation report and, optionally, save a copy (the XOsoft Engine now is installed on all selected servers or cluster nodes)



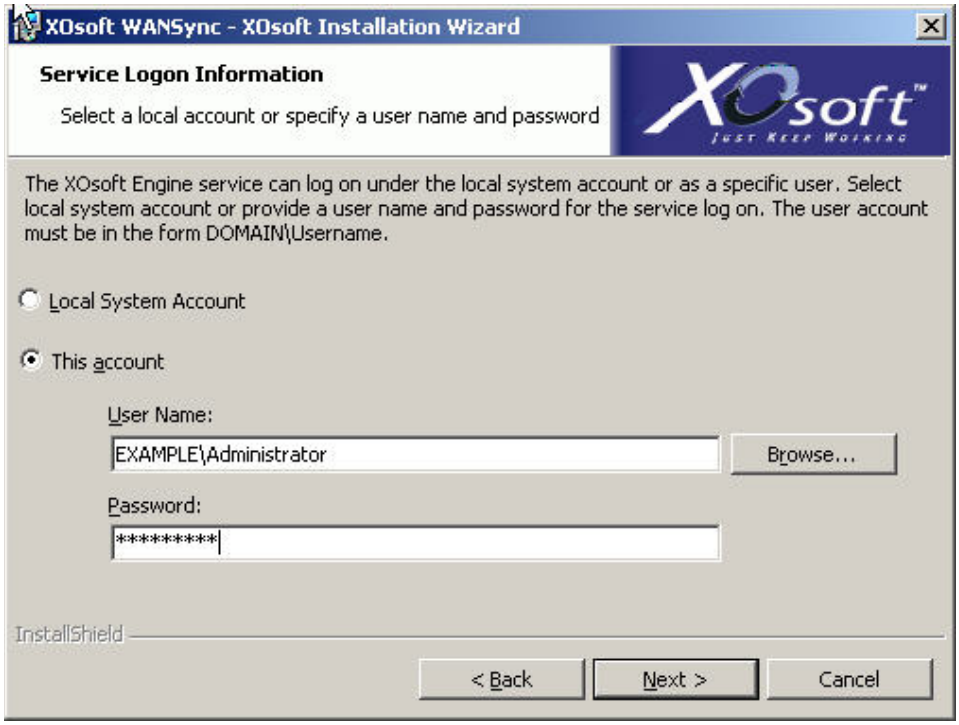
Master Server

To install on the master server:

1. If you did not use the Remote Installation Wizard, install WANSyncHA on the master server.

   Note: When installing WANSyncHA, use the log on account as described in *Requirements*.

If you installed under a different account than required, you can change it any time using the Windows services console: find the XOsoft Engine service and change the log on account. Then restart the service to apply the change.



2. If you have file level antivirus software installed, exclude the WANSyncHA installation directory from antivirus protection.
3. If the master server is a cluster, perform steps 1 and 2 on all nodes. You do not need to switch over the MS IIS group during installation.

Replica Server

To install on the replica server:

1. If you did not use the Remote Installation Wizard, install WANSyncHA on the replica server.

   Note: When installing WANSyncHA, use the log on account as described in *Requirements*.

   If you installed under a different account than required, you can change it any time using the Windows services console: find the XOsoft Engine service and change the log on account. Then restart the service to apply the change.
2. If you have file level antivirus software installed, exclude the WANSyncHA installation directory from antivirus protection.
3. If the replica server is a cluster, perform steps 1 and 2 on all nodes. You do not need to switch over the MS IIS group during installation.

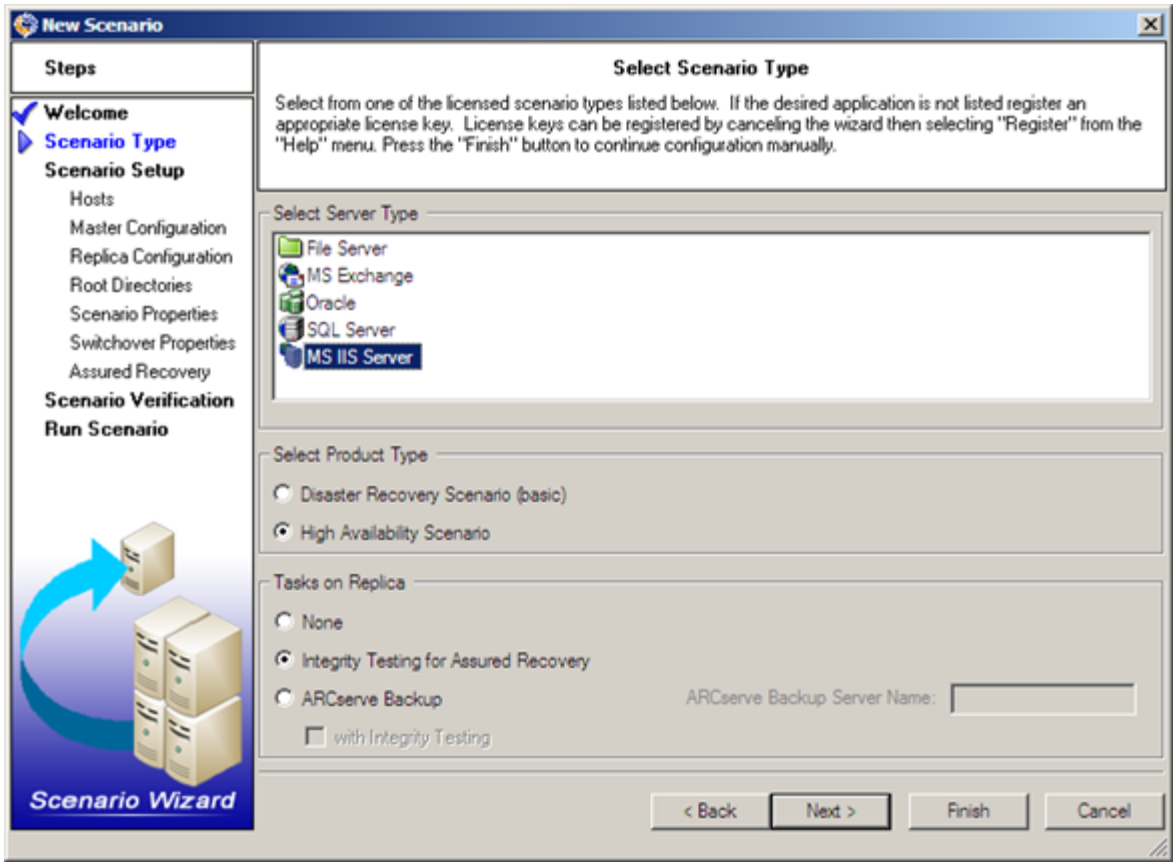
Configure a Replication Scenario

The following subsections describe how to create and configure a replication scenario.

Create a New Scenario

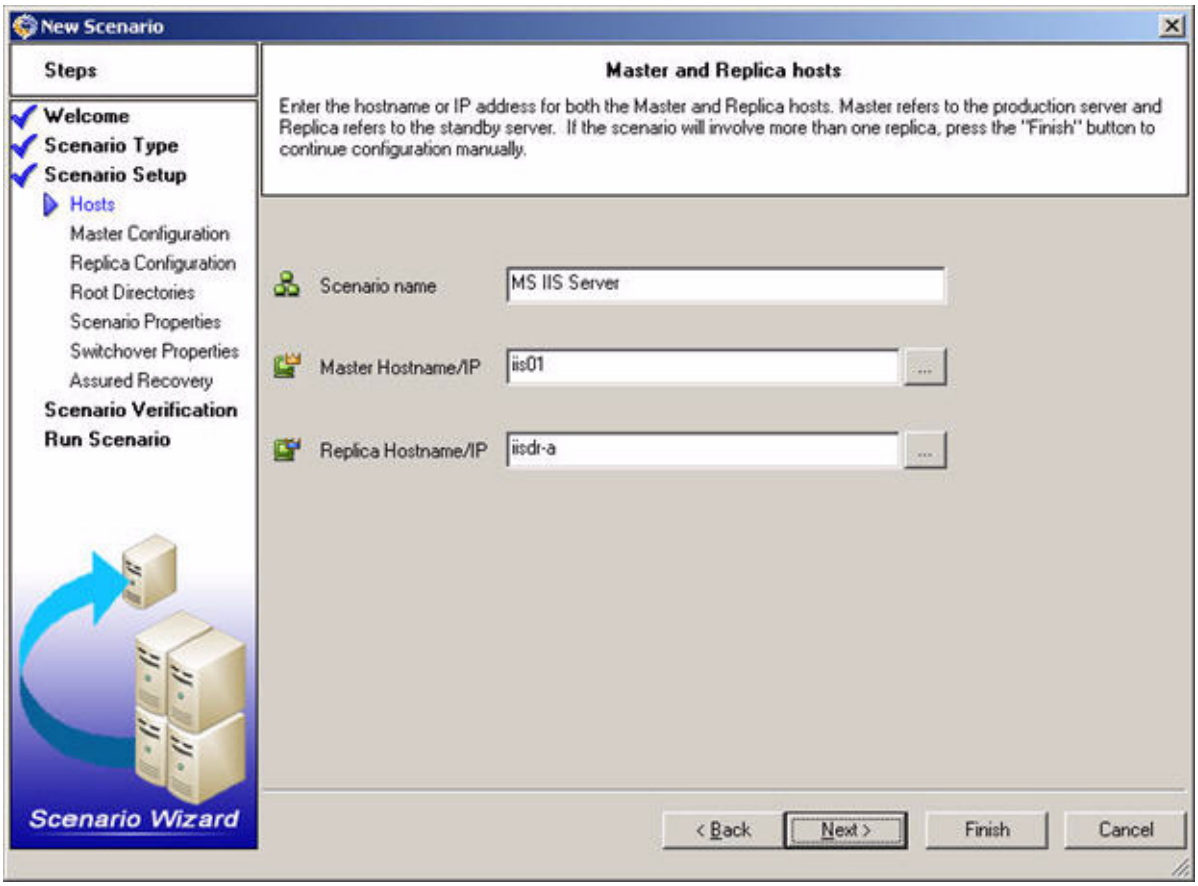
1. Open WANSync Manager. From the File menu select *New* or click the New Scenario button.
2. At the Welcome step click Next to *Create New Scenario*.
3. At the Scenario Type step select *MS IIS Server* and *High Availability Scenario* and, optionally, *Replica Integrity Test for Assured Recovery*.

   Note: Learn more about Assured Recovery and how it can help ensure success through automatic testing. Please visit the Products menu at www.caxosoft.com or review the *WANSync User Guide* for more information.

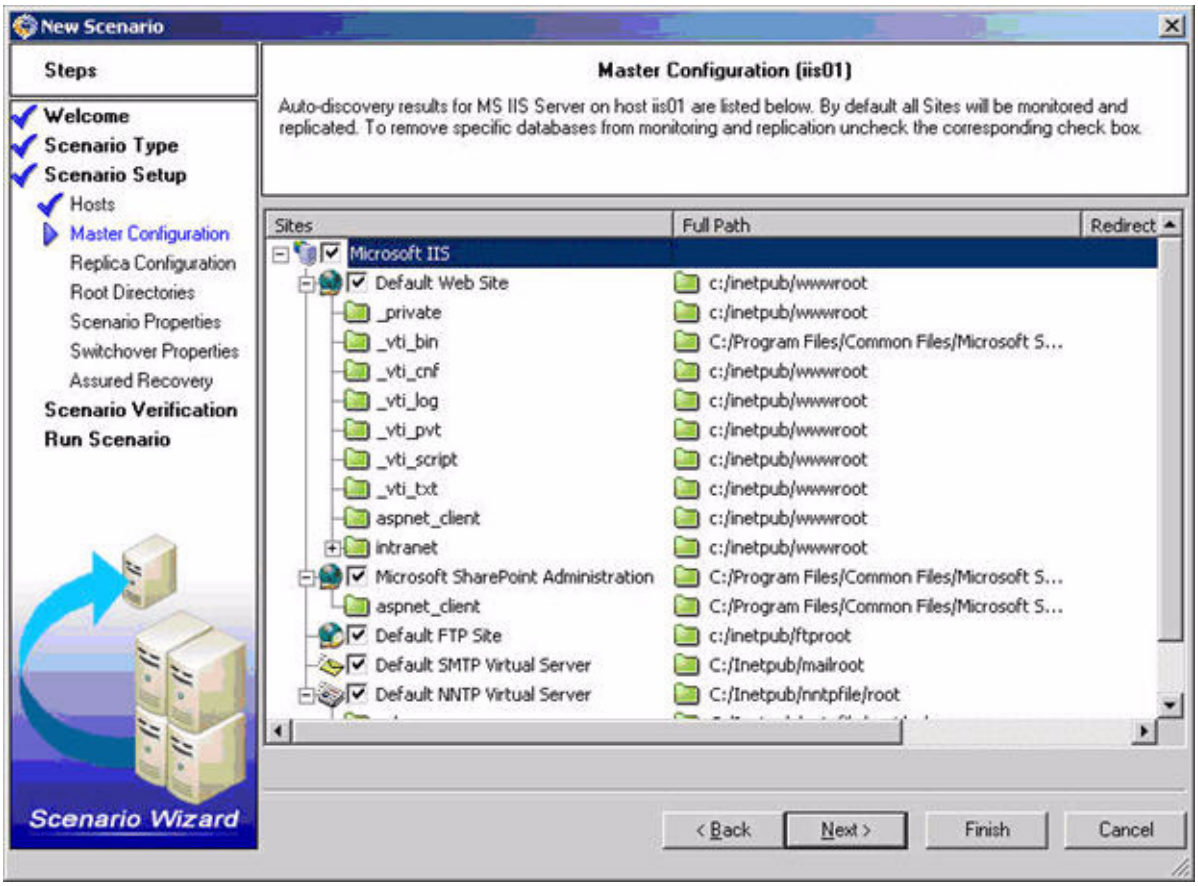


4. During the Hosts step, name the scenario and input the server names for the master and replica hosts.

Note: If either server is a MSCS cluster, enter the cluster resource virtual server network name (or IP address) as the master and/or replica name.

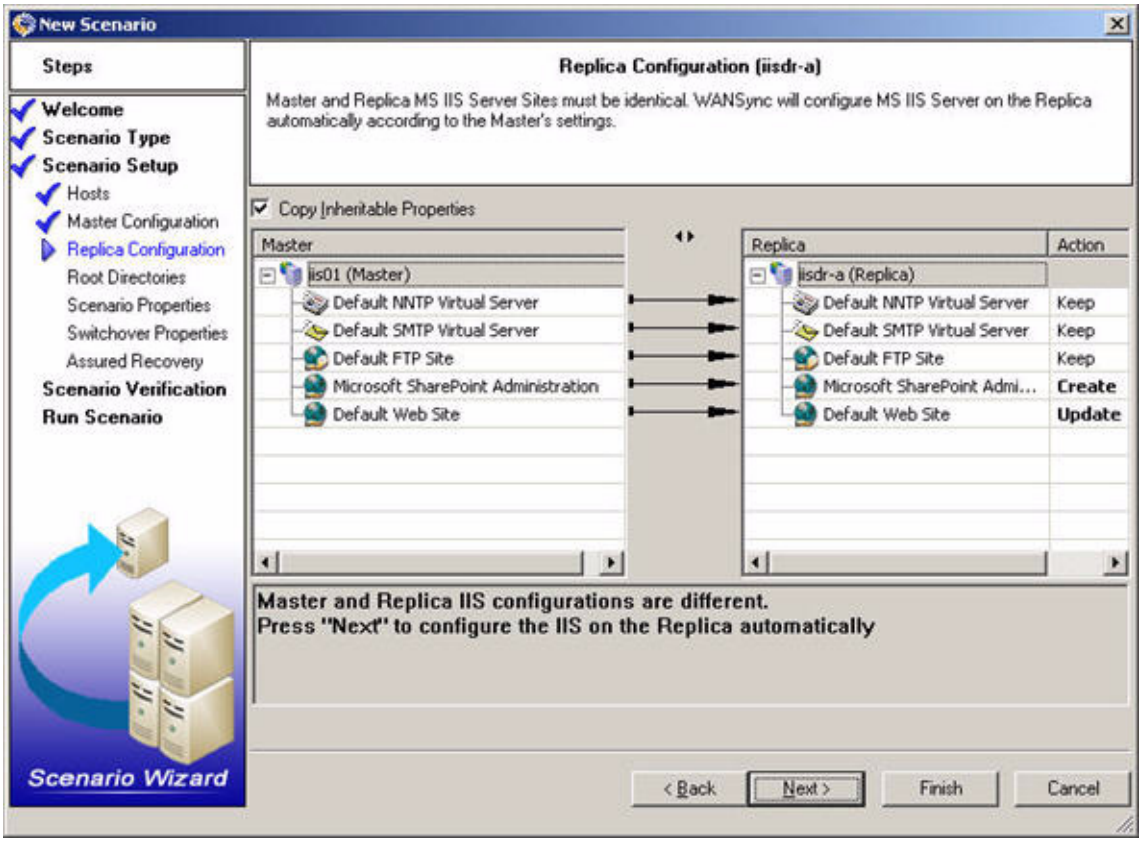


5. At the Master Configuration step, WANSyncHA displays the sites on the master server. These are the sites that will be replicated and protected. At this step you also have the option to exclude specific sites from replication and monitoring.

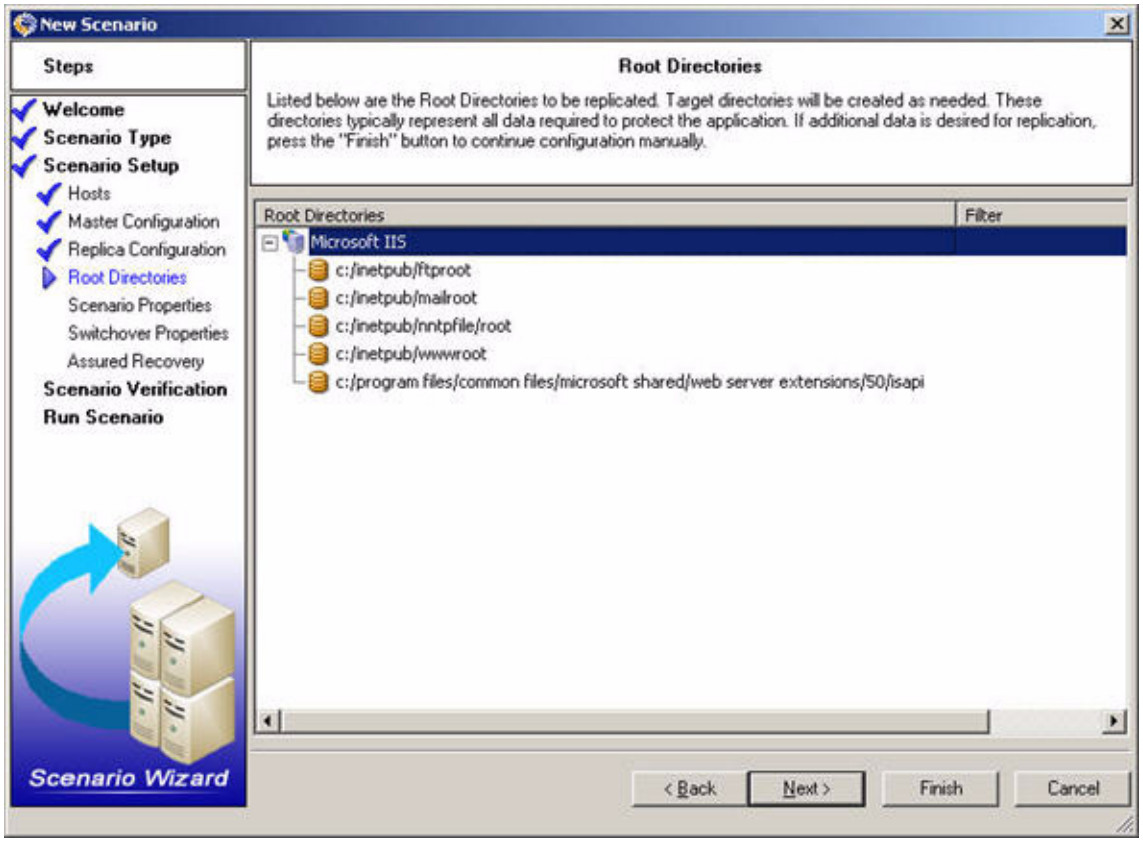


6. Review the changes that will occur during automatic configuration on the replica IIS server. The Copy inheritable properties option copies all settings that are inherited by virtual directories from the parent site. This option is selected by default and is the recommended option for most cases. Click Next to start the replica configuration process.

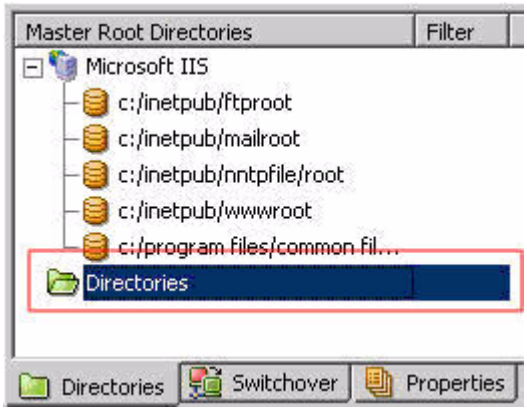
For information on how to repeat the autoconfiguration process after the wizard completes, see *Autoconfigure MS IIS Using the ws_iis2iis Utility*.



7. The Root Directories step displays the data to be replicated. Click the Next button to continue.

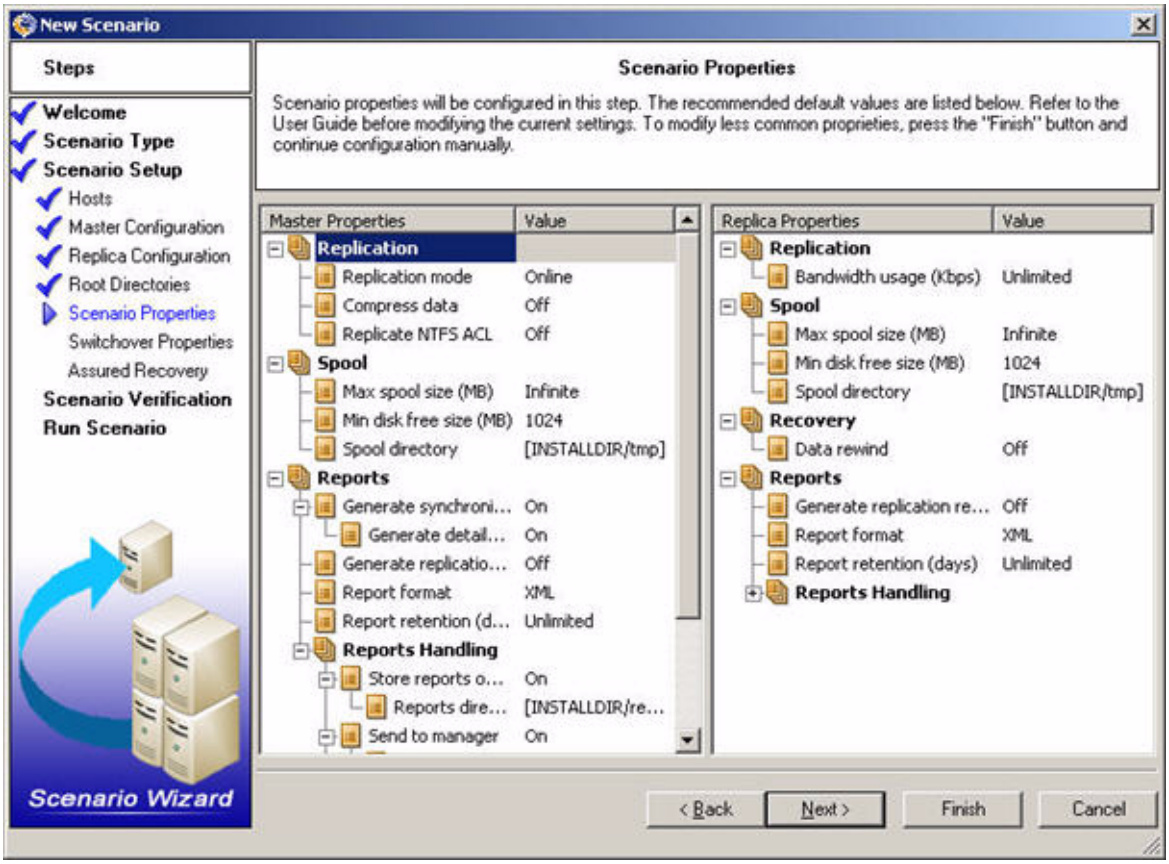


Note: You can add additional files or folders to the replication after running this wizard. Follow the prompt to run the scenario later then double click on *Directories* under the Directories tab.



8. The Scenario Properties step allows you to configure additional properties. If you use NTFS ACL's (permissions) with domain accounts for user access control, we recommend choosing the *Replicate NTFS ACL* option. Otherwise, click Next to proceed.

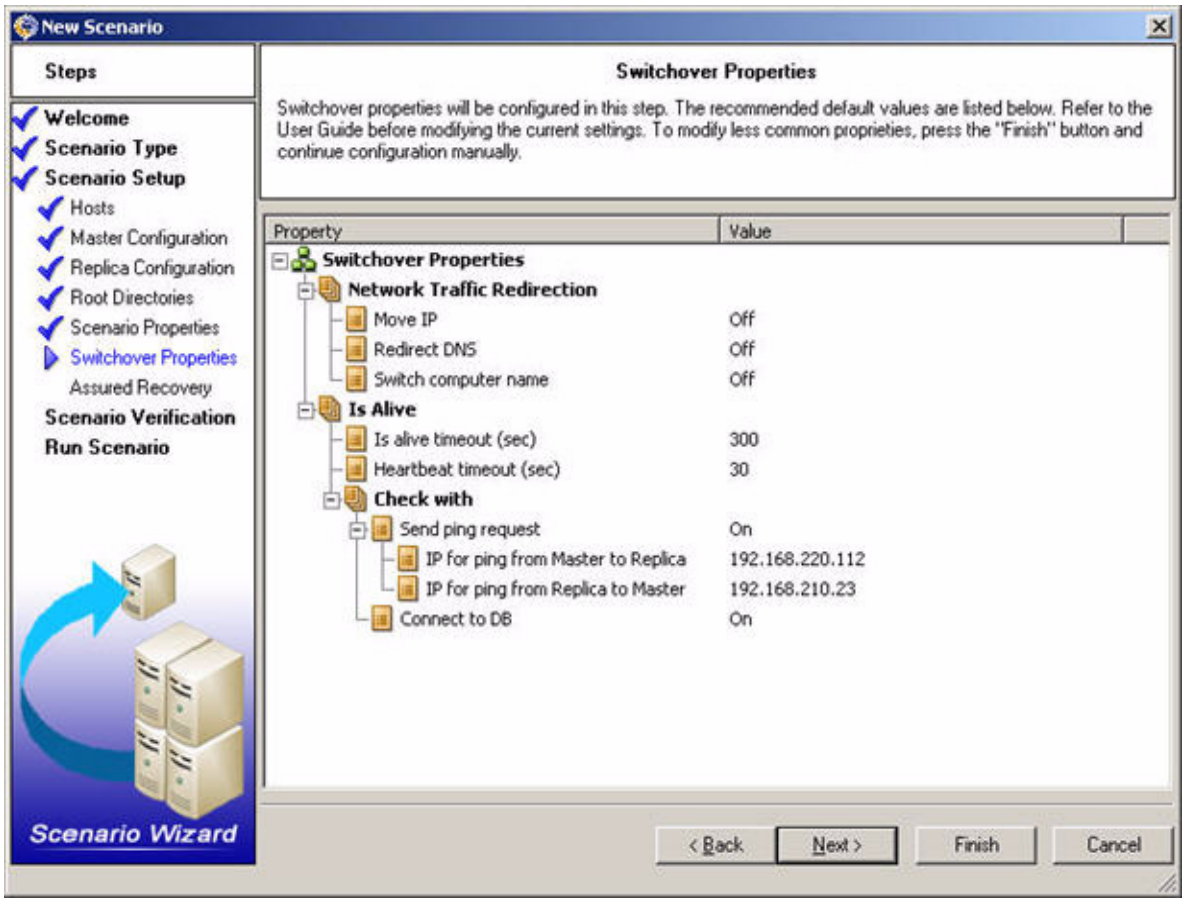
   Note: You can modify all the settings in this pane after the scenario is created. However, before changing any Spool properties (which are configured here), please review *Spool Settings* for configuration details.



9. The Switchover Properties step allows you to modify switchover parameters. At this step you must choose a redirection method that suits your needs, or click Finish to specify custom scripts manually as the redirection method. By default, no redirection method is set to on. If you did not review the section *Determine Which Redirection Method to Use*, please do so now and choose the one that is appropriate for your configuration. In most cases, however, Redirect DNS or Move IP work best.

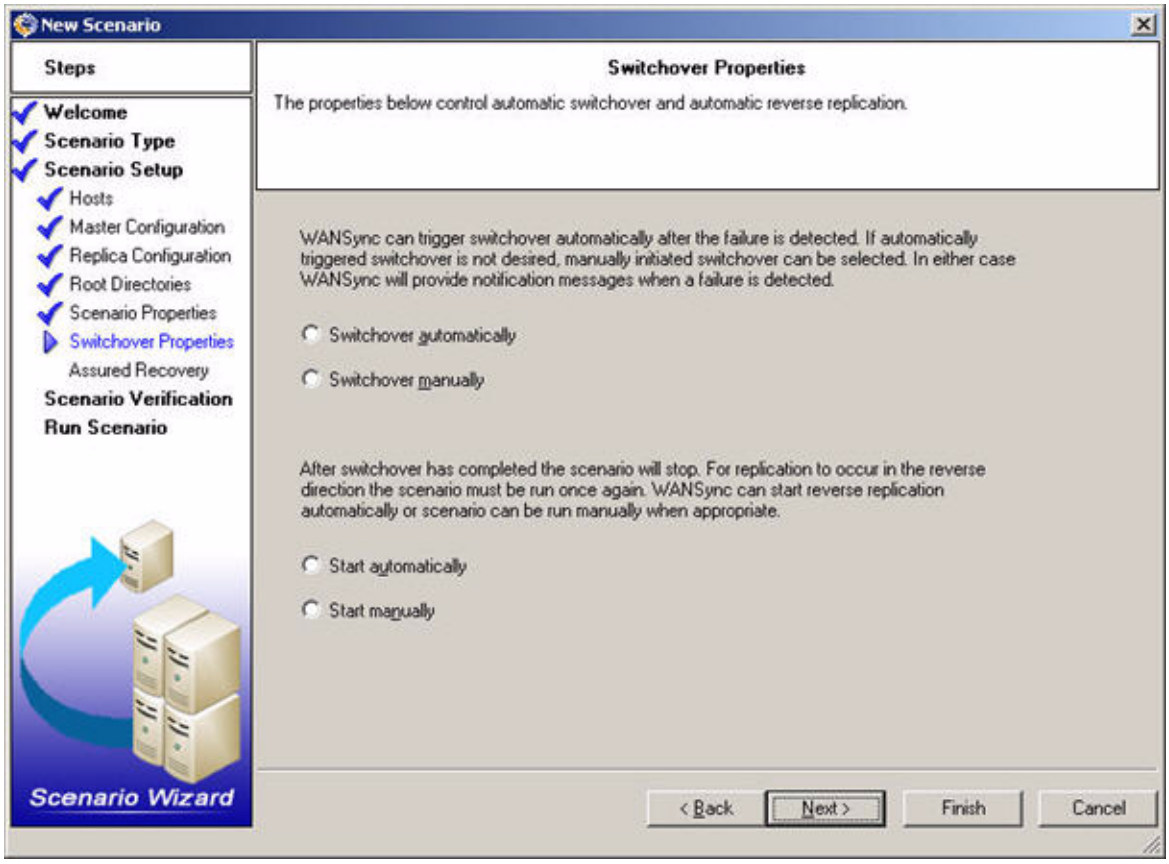
   Note: For users planning to use automatic switchover, please note that the *Is alive timeout (sec)* setting controls how long to wait after a failure is detected before triggering switchover.

If you intend to use Move IP as the redirection method, please see *Move IP Redirection*.



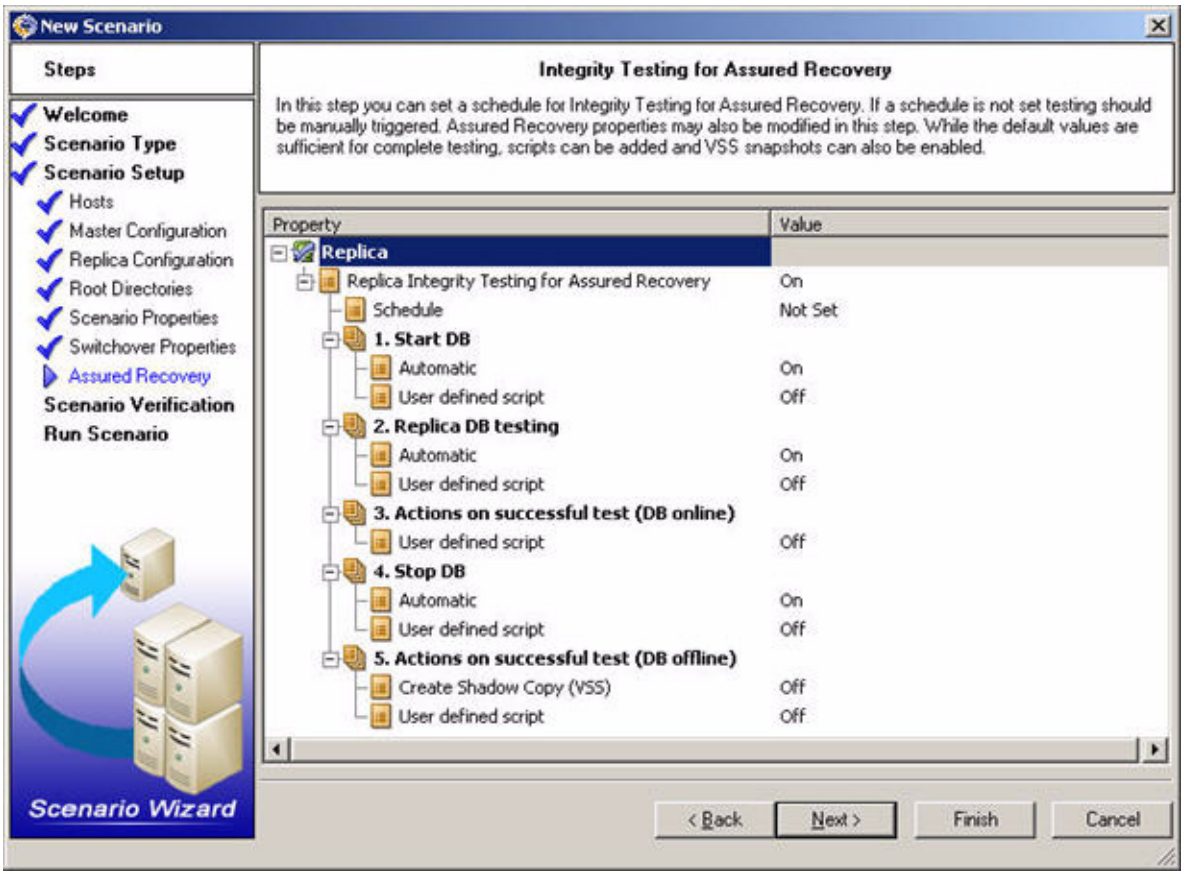
10. The last step in Switchover Properties defines which steps are triggered automatically by WANSyncHA or triggered manually by the Administrator. Select the desired setting for each option and then click the Next button.

    Important! It is not recommended to use automatic reverse replication with IIS scenarios. (see *Automatic Switchover and Reverse Replication*).



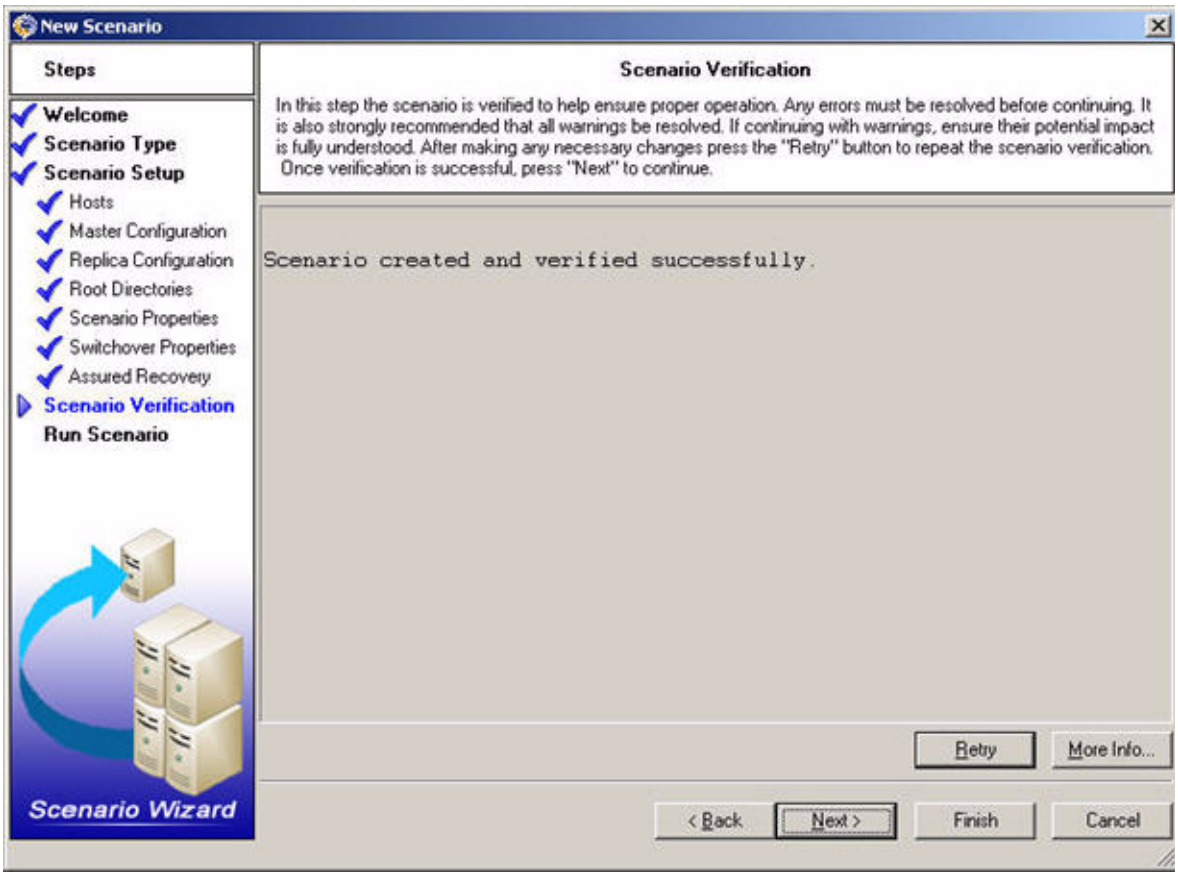
11. The Assured Recovery step is presented only if you selected this option in the Scenario Type step.

Note: If scheduled testing is desired, double-click on the value for *Schedule*: the Assured Recovery hours screen opens allowing you to set a schedule for testing.



12. Scenario Verification checks many different parameters between the master and replica and servers to ensure a successful switchover. If any errors are reported you cannot continue until they are resolved. To retry verification click the Retry button. Once the scenario is verified successfully, click Next to continue.tion is complete: All modifications during synchronization are replicated.

Important! Although the software allows you to continue with warnings, it is not recommended to do so. Resolve any warning situations before continuing to ensure proper operation of the application.

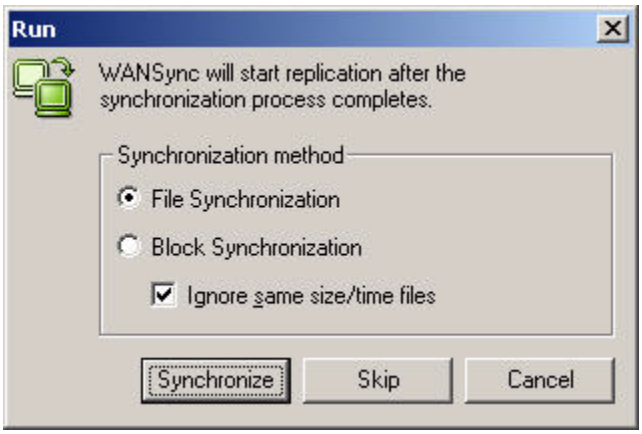


Run a Scenario from Outside the Wizard

1. Select the Run button on the WANSync Manager tool bar or select *Run* from the Tools menu.
2. Before initiating synchronization and replication, WANSyncHA verifies your scenario configuration. When verification is complete, WANSync Manager displays the message: *Are you sure you want to run scenario "scenario_name?"* The top pane displays any warning and error messages resulting from verification.

   Note: Scenario Verification checks many different parameters between the master and replica and servers to ensure a successful switchover. If any errors or warnings are reported you should not continue until they are resolved.

3. Click OK to run the scenario. The Run screen is displayed:



4. Leave the File Synchronization method with the *Ignore Same Size/time Files* option checked.

   Important! File synchronization is best suited for large numbers of relatively small files. If you want to learn more about other synchronization methods, please see the *WANSync User Guide.*

5. Click the Synchronize button. Synchronization can take a while, depending on database size and network bandwidth between the master and replica. You will receive the following message in the event window when the synchronization is complete: *All modifications during synchronization are replicated.*

At this point, real-time replication is operational and the high availability solution is installed and active.

Autoconfigure MS IIS Using the ws_iis2iis Utility

The WANSyncHA autoconfiguration process for web sites and settings only runs once during scenario creation in order to conserve bandwidth and server resources. If at any point in the future you want to refresh the IIS configuration on the replica, the ws_iis2iis utility is provided for this purpose. You can run this utility at the server or site level. You can also use the utility to update the replica configuration for newly added sites (in this case you should also rerun autodiscovery from the Directories tab in the WANSync Manager).

The utility is located in the WANSyncHA installation directory. You can use the utility manually or scripted for a scheduled operation. Run ws_iis2iis without any switches for a command line reference.

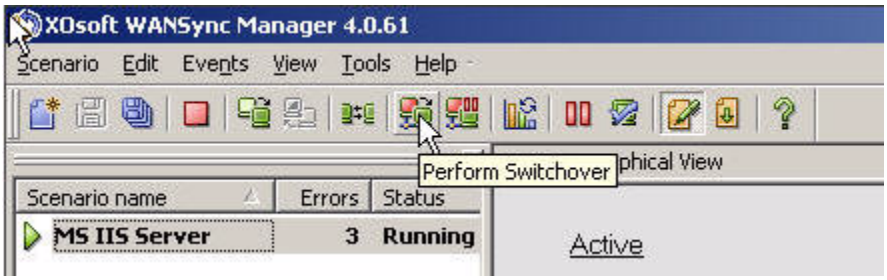
Chapter 3: Switching Over and Switching Back

This chapter describes the switchover and switchback processes. After completing synchronization, you can initiate switchover and switchback.

Switchover

To initiate switchover:

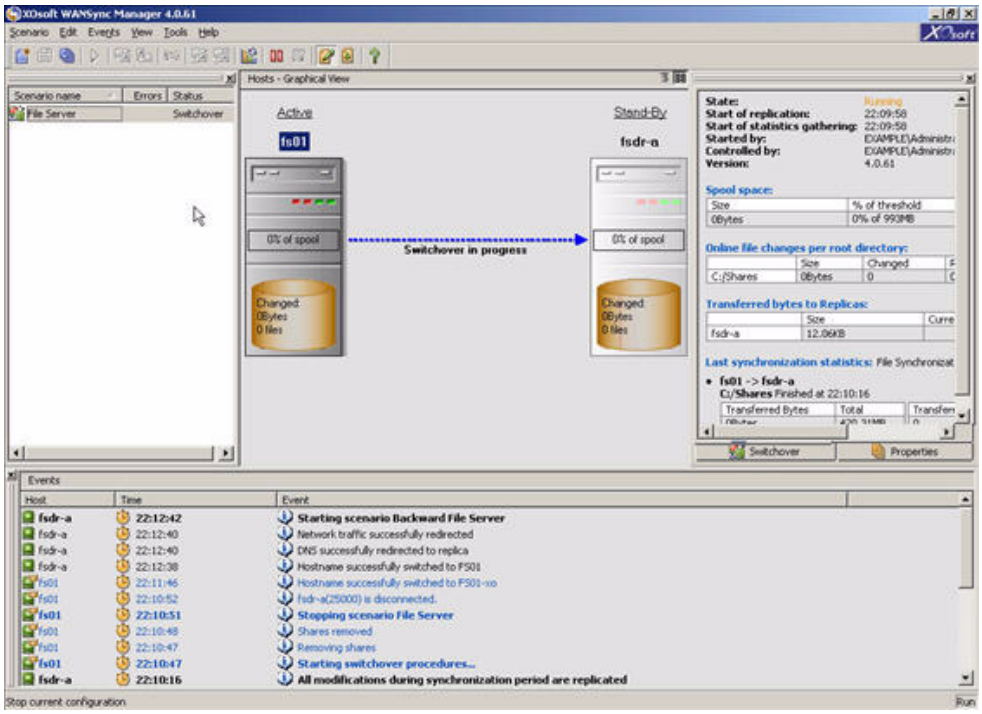
1. Open WANSync Manager and select the desired scenario.
2. Click on the Perform Switchover button or select *Perform Switchover* from the Tools menu.



3. Click OK on the Perform Switchover confirmation window.

   This procedure initiates a switchover from the master server to the replica server. Detailed information about the switchover processes is located in the Events pane during switchover.

Important! After switchover completes the scenario stops. The only case in which the scenario may continue to run after switchover is when automatic reverse replication is turned on. For more information, see *Automatic Switchover and Reverse Replication*.



Switchback

To initiate switchback:

1. Ensure that both master and replica servers are available on the network and the WANSync service (XOsoft Engine) is running.
2. From WANSync Manager, choose the desired scenario.
3. Skip this step if the backward scenario is already running. If the backward scenario is not running, select *Run* to start the scenario: WANSyncHA detects that a switchover has occurred and prompts you that it is running a backward scenario.
4. If resynchronization was required wait for it to complete. You will receive the following message in the Event window: *All modifications during synchronization are replicated*.
5. Click on the Perform Switchover button or select *Perform Switchover* from the Tools menu and then click OK on the Perform Switchover confirmation window.

After switchback is completed, you can again run the scenario in its original (forward) state. In order to avoid resynchronization after a successful switchover, you can opt to use the *Run Reverse Replication Scenario Automatically* option (see *Automatic Switchover and Reverse Replication*).

Appendix A: WANSyncHA Tips

This chapter provides you with helpful information concerning the application.

Spool Settings

The WANSyncHA spool is a folder on disk where data to be replicated is backed up (i.e., spooled) if bandwidth is not sufficient to transfer the amount of changes in real-time. Data can spool due to temporary network disconnections, network congestion, or simply because the network bandwidth is not sufficient to transfer the amount of data changing over on the server.

In addition to storing changes waiting on available bandwidth, spool space is also used as part of the normal synchronization process. Thus, some spool build up during synchronization is normal.

Place the WANSyncHA spool folder on a drive with relatively low use such as a dedicated volume or boot/system volume. Do not place the spool folder on a volume containing frequently accessed system (OS), user, or application data. Examples include volumes containing databases, shared files, or the system pagefile. By default, the spool folder is located in the tmp folder under the WANSyncHA installation directory. The spool parameters, located in the properties tab (on both master and replica) or set with the New Scenario Wizard, determines how much disk space is available for the spool. In most cases the default values are sufficient. However, if you choose to change this value, it should be at least 10% of the total dataset size. For example, if you are replicating 50GB of data on a server you should ensure that at least 5GB of space is available for spool. Please note that this space is not pre-allocated.

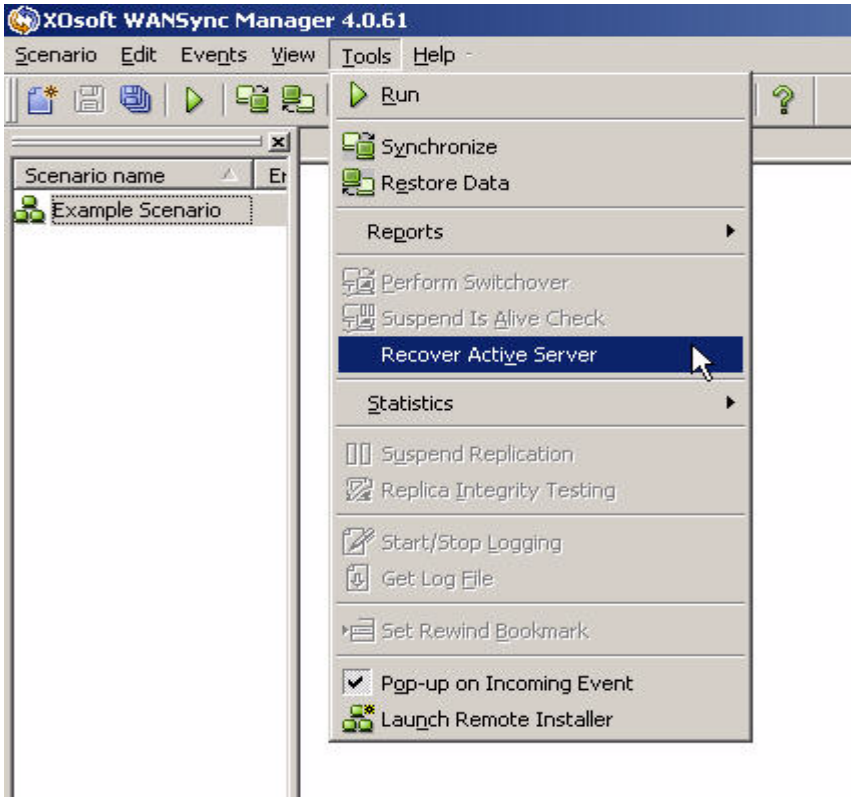
Important! If you change the spool location, please remember to remove the new path from file level antivirus scans: both scheduled and real time.

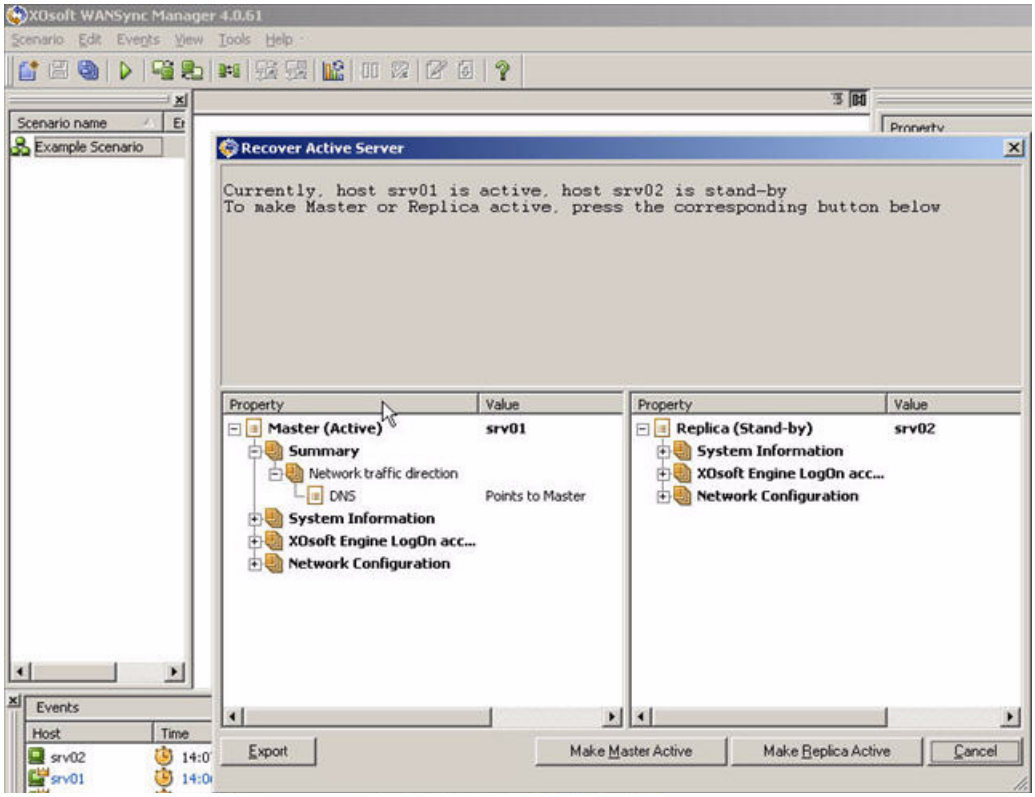
Recover Active Server

In certain circumstances, it may be necessary to forcibly make the master or replica server the active server without completing the data synchronization process. For example, if switchover occurred but no data was changed on the replica server. In this case you may even have newer data on the master server making it undesirable to synchronize data from the replica to the master server. WANSyncHA allows for this option through a process called Recover Active Server. To use this option, ensure that the scenario is stopped, and select *Recover Active Server* from the Tools menu.

Important! While this option is the right choice in many situations, use it with caution. If used improperly data loss can occur. Normally WANSyncHA will not allow switchover from one host to another until all data is synchronized. It is designed this way so users are not redirected to an out of date data set that then overwrites what may be a more current data set. When using Recover Active Server, WANSyncHA is forcing users to one server or the other with no regard as to which server has the correct data set. Thus, as an administrator, you must manually ensure that the server you are making active has the most up to date data set.

Recover Active Server is not available if you are using the Switch Computer Name redirection method.





Select either *Make Master Active* or *Make Replica Active* depending onto which server you want to force the active role.

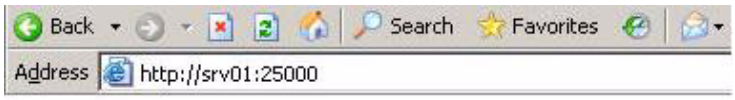
Important! If a legitimate switchover in a disaster situation occurs and users are redirected to the replica server for any period of time, it is important to replicate all changes on the replica back to the master before making the master server active. Using *Recover Active Server* in such a situation results in loss of data.

Read Only Web GUI

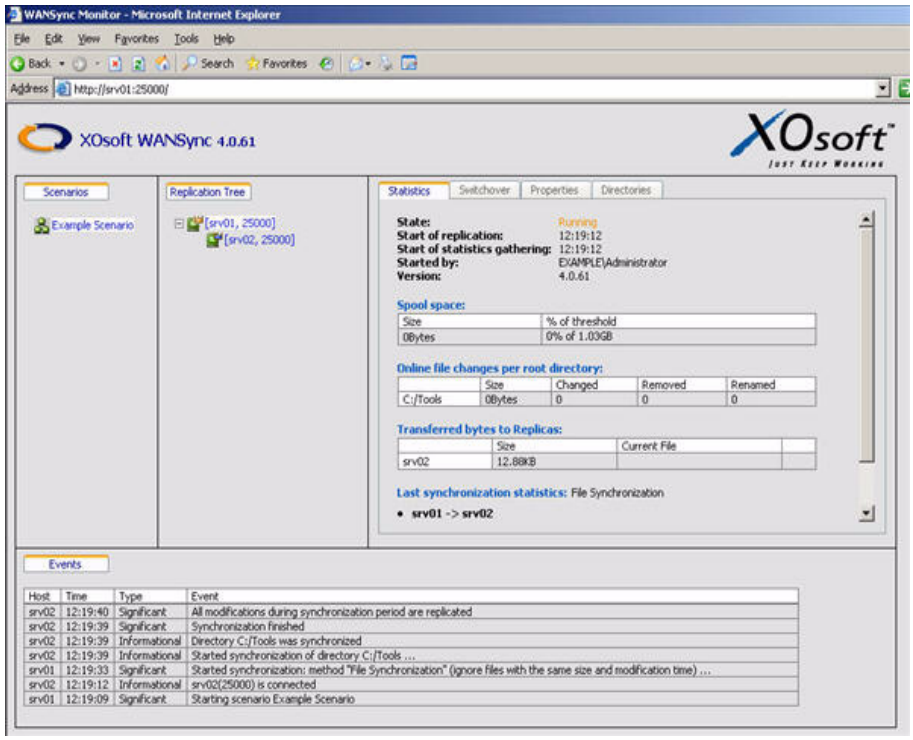
The primary WANSync Manager may only be used by one Administrator at a time. Opening the GUI locks it for the current user making simultaneous use impossible. This is required to prevent conflicts. To allow simultaneous monitoring by any number of administrators WANSyncHA also offers a read only Web GUI.

To access the web GUI:

1. Open your browser to http://masterservername:25000.
2. Enter a user account and password with administrative permissions on the master server.



Important! There is no need to refresh the browser; the GUI refreshes automatically. You can monitor all parameters, statistics, and events from this window.



Appendix B: Automatic Switchover and Reverse Replication

This chapter describes the automatic (triggered) switchover and automatic reverse replication processes.

Automatic Switchover

Triggered (automatic) switchover is in all ways identical to manual switchover performed by the administrator. Automatic switchover is triggered by a resource failure on the master server rather than by an administrator manually initiating the switchover by clicking the Perform Switchover button. Server ping response, application service status, and database connectivity are monitored. The timeout parameters are configurable and are more extensively covered in the *WANSync User Guide*.

Automatic Reverse Replication

When this feature is off, to start reverse replication after a switchover has occurred, click the Run button. The benefit to this feature is, if both the master and replica servers were online and connected during switchover, resynchronization in the reverse direction is not required. Resynchronization involves comparing the data on the master and replica servers to determine which changes to transfer before real-time replication starts; this can take some time. If automatic reverse replication is turned on, and both servers were online during switchover, replication is reversed without the need for resynchronization. This is the one situation in which resynchronization is not required.

Best Practice

It's not recommended to use automatic reverse replication with IIS scenarios: WANSync is unable to validate that your replica data is good before overwriting the data on the master server (after switchover). In database scenarios (SQL, Exchange, etc.) this option is safe because WANSync validates that the replica databases are good before overwriting data on the master server. With IIS scenarios no such protection exists and as such this option is not recommended. Use only if you fully understand the possible implications.

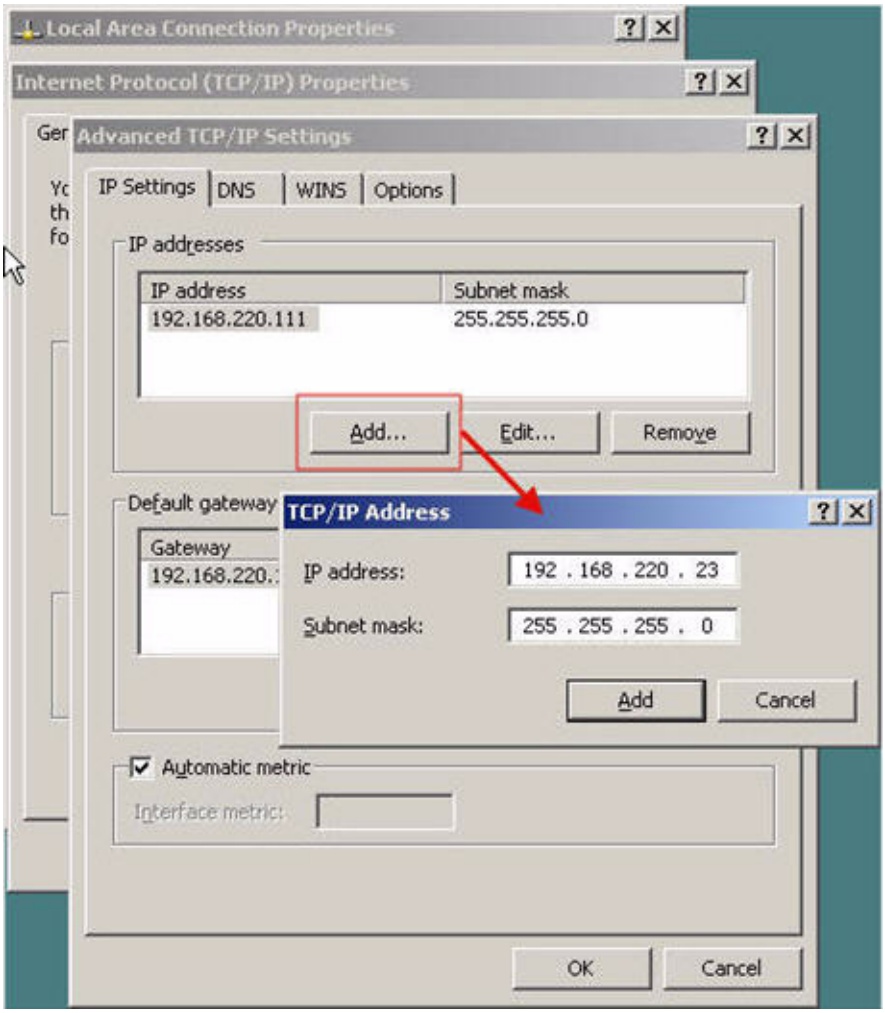
Appendix C: Move IP Redirection

This section describes how to add Move IP redirection to a high availability scenario. Use this method only when both servers are on the same IP subnet.

Move IP on the Master Server

Before configuring the scenario, add an additional IP address to the master host, (which is denoted as *WS-IP* in the following steps). If you have already configured your scenario go ahead and add this IP address; special steps for this situation are listed below. This new IP address is used for WANSync internal communication and replication. This is necessary since the current production IP address is not available on the master after switchover -- it switches to the replica server.

Note that in the following screen shot, the WS-IP IP address is 192.168.220.23 and the current production server IP address is 192.268.220.111.



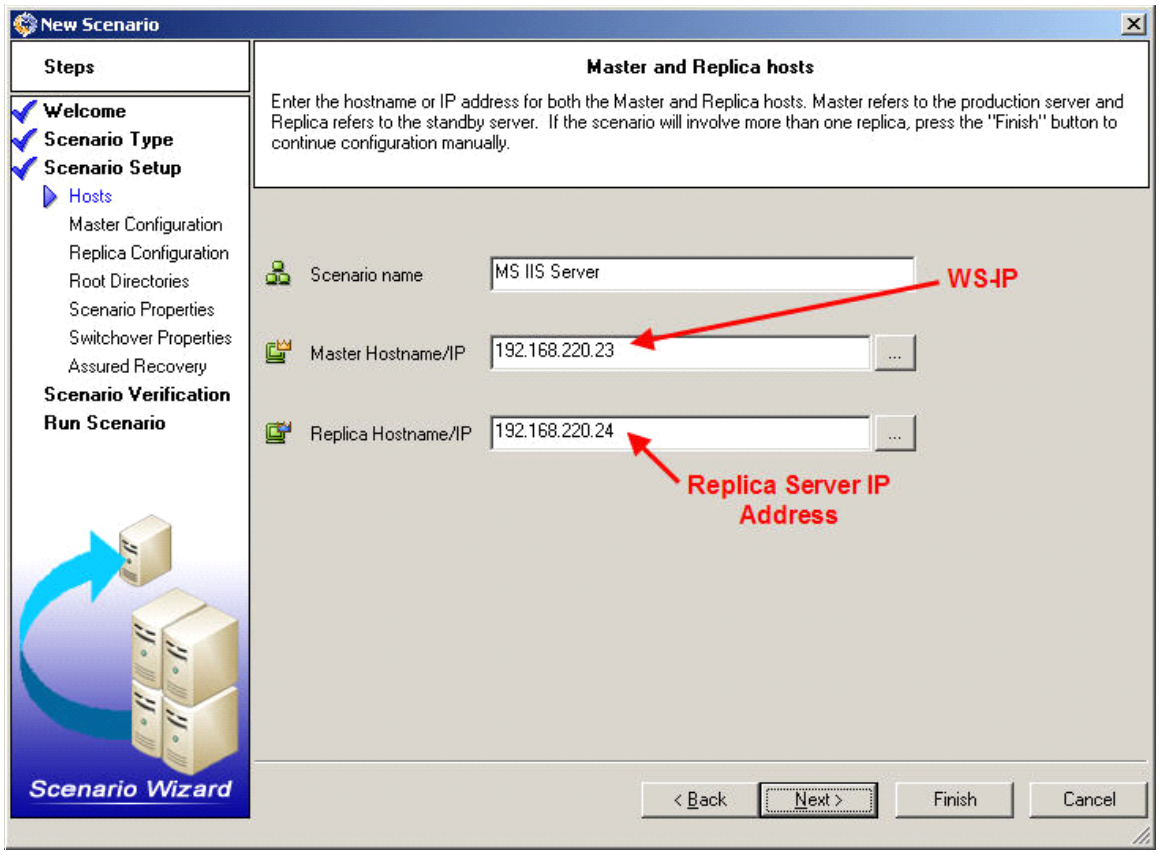
Move IP on the WANSync Manager

This subsection details Move IP redirection on the WANSync Manager.

For New Scenarios

To implement Move IP with new scenarios:

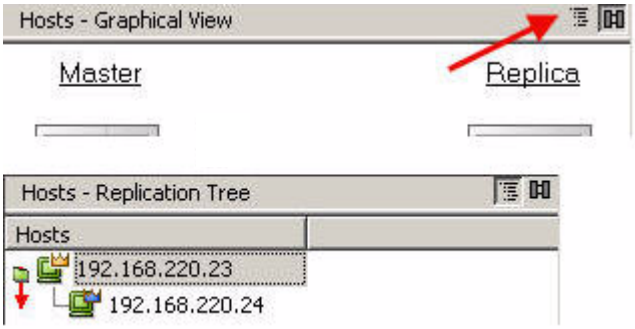
During the initial run of the Wizard, enter the WS-IP and replica IP addresses instead of the server names.



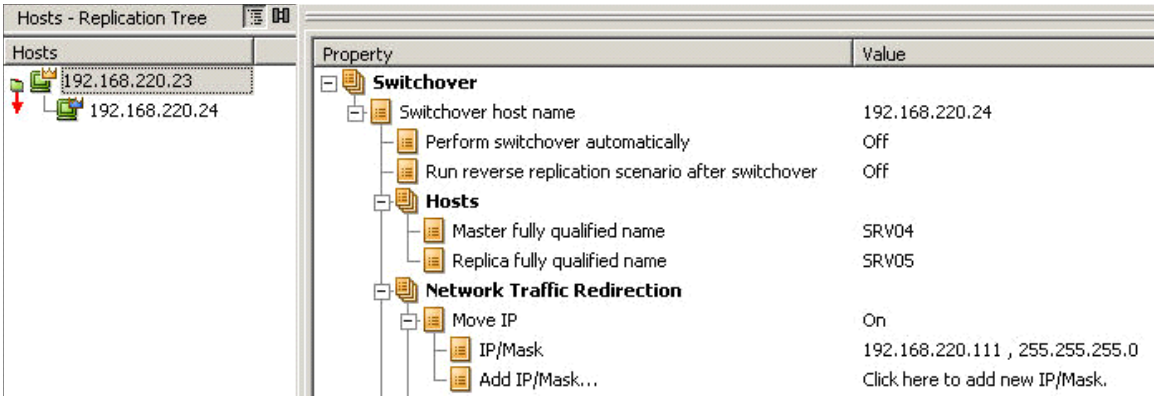
For Existing Scenarios

To implement move IP with existing scenarios:

1. If the Hosts pane is in Graphical View switch to Replication Tree view by clicking the left button in the top right corner of the pane.



2. Right click on the master host name and choose *Rename*. Then enter the WS-IP address.
3. Select the Switchover tab and then select the replica server as the switchover host.
4. Set the *Move IP* option to On. Ensure that the IP address under *Move IP, IP/Mask* matches the production server IP address: this is the IP address that will switch over. If you are moving more than one IP address you can add multiple production IP addresses by selecting *Click here to add new IP/Mask*.



Cluster Move IP

Using Move IP redirection with a clustered master (MSCS with shared storage) requires you to add an additional IP resource to the master File Server resource group. This section describes Move IP redirection from a master cluster to a single server replica.

Note: If both master *and* replica are clusters there are special configuration issues involved in the Move IP redirection process that are not detailed in this guide. For a cluster-cluster scenario, use Redirect DNS or contact technical support to receive detailed instructions and guidance.

On the Master Cluster

To use cluster move IP on the master cluster:

1. Open the Cluster Administrator.
2. In the Master Cluster IIS Resource Group, create a new IP resource and name it *WS-IP*.
3. Bring this resource online and verify it is visible from the replica via the ping command. This new IP address is used for WANSyncHA internal communication and replication. This is necessary since the current production IP address is not available on the master cluster after switchover -- it switches to the replica server.

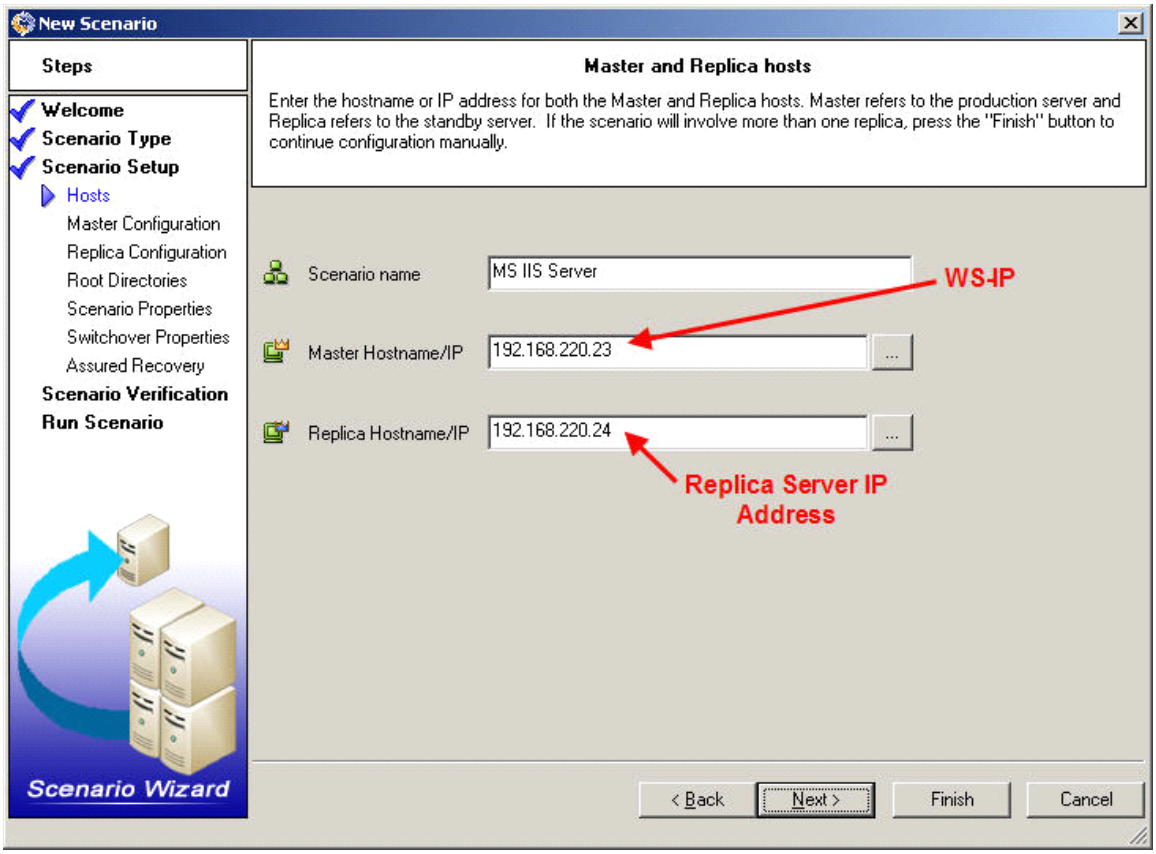
On the WANSync Manager

This subsection details Cluster Move IP redirection on the WANSync Manager.

For New Scenarios

To implement cluster Move IP with new scenarios:

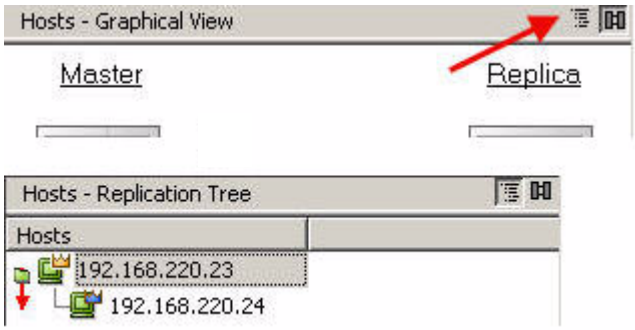
During the initial run of the Wizard, enter the WS-IP and replica IP addresses instead of the cluster virtual server names.



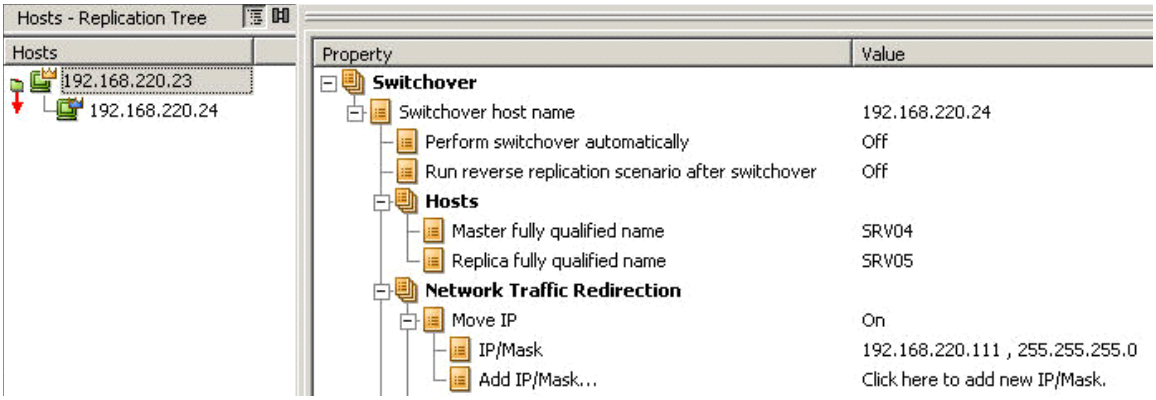
For Existing Scenarios

To implement cluster move IP with existing scenarios:

1. If the Hosts pane is in Graphical View switch to Replication Tree view by clicking the left button in the top right corner of the pane.



2. Right click on the master host name and choose *Rename*. Then enter the WS-IP address.
3. Select the Switchover tab and then select the replica server as the switchover host.
4. Set the *Move IP* option to On. Ensure that the IP address under *Move IP, IP/Mask* matches the production server IP address: this is the IP address that will switch over. If you are moving more than one IP address you can add multiple production IP addresses by selecting *Click here to add new IP/Mask*.



Appendix D: Switch Computer Name Redirection

This chapter describes the method of redirection in which you switch the computer name.

Automatic

When possible during switchover, WANSyncHA gracefully renames the master host to *masterhostname-XO* and assigns its original name to the replica server. This step prevents name conflicts since the master's name is now assigned to the replica server. In this graceful case, if automatic reverse replication is set to on, WANSync starts the backward scenario automatically. If automatic reverse replication is set to off, run the scenario again manually by selecting the Run button or choosing *Run* from the Tools menu. Once the backward scenario has run and synchronization is complete you can click the Perform Switchover button to switch back.

Manual

If the master server was offline or otherwise unavailable during switchover WANSyncHA may not be able to rename the master to *masterhostname-XO*. In this case, it is necessary to perform the following steps manually before bringing the master back onto the network and starting the backward scenario:

1. Unplug the master server from the network and log on as a local Administrator.
2. Plug the master back into the network.
3. Rename the master server to *masterhostname-XO*. For example, name the master server *SRV-XO* and move it to a workgroup.
4. Join the master server back to the domain with the temporary name *masterhostname-XO*.

5. If automatic reverse replication is set to on, WANSync starts the backward scenario automatically; if it is set to off or the scenario was stopped, run the scenario again manually by selecting the Run button or choosing *Run* from the Tools menu. Once synchronization from replica to master is complete you can click the Perform Switchover button to switch back.

Appendix E: Replication in a Workgroup Environment

WanSyncHA can replicate IIS data between two servers in a workgroup environment. Since servers in a workgroup do not have access to a common security database, it is necessary to create identical service accounts locally on both servers and assign them identical passwords. If anonymous access is used, configure all websites running on both servers to use the same username/password combination for anonymous access. Failure to do this results in an authentication window when trying to access web sites on the replica server.

Configure Service Accounts

To configure service accounts:

1. Create identical user accounts on both servers.
2. Assign identical passwords to both accounts.
3. Configure this as the account used for anonymous access in the properties of each web site for which anonymous access is enabled.
4. If you want to use the default *IUSR_<computername>* account on both servers for anonymous access, ensure that you assign identical passwords to both accounts, and uncheck the "Allow IIS to control password" selection in the Properties > Directory Security > Authentication Methods section of each web site for which anonymous access is enabled.

Important! If the IIS scenario is configured to replicate ACLs, a view of the security properties of the folder(s) containing web site content on the replica shows an unresolved SID – this is by design and can be ignored.

Additional Resources

The following Microsoft knowledge base articles discuss how to configure web site authentication:

- **For IIS 5.0:** *How To Configure IIS 5.0 Web Site Authentication in Windows 2000* - http://support.microsoft.com/kb/310344
- **For IIS 6.0:** *How To Configure IIS Web Site Authentication in Windows Server 2003* - http://support.microsoft.com/kb/324274

Index

R

S

W

X